

5.0

TREND MICRO™ Endpoint Encryption

Installations- und Migrationshandbuch

Umfassende Endpunktverschlüsselung für gespeicherte Daten



Trend Micro Incorporated behält sich das Recht vor, Änderungen an diesem Dokument und dem hierin beschriebenen Produkt ohne Vorankündigung vorzunehmen. Lesen Sie vor der Installation und Verwendung des Produkts die Readme-Dateien, die Anmerkungen zu dieser Version und/oder die neueste Version der verfügbaren Dokumentation durch:

http://docs.trendmicro.com/de-de/enterprise/endpoint-encryption.aspx

Dokument-Nr.: APGM56403/140410

Release-Datum: Dezember 2014

Geschützt durch U.S. Patent-Nr.: Zum Patent angemeldet.

In dieser Dokumentation finden Sie eine Einführung in die Hauptfunktionen des Produkts und/oder Installationsanweisungen für eine Produktionsumgebung. Lesen Sie die Dokumentation vor der Installation und Verwendung des Produkts aufmerksam durch.

Ausführliche Informationen über die Verwendung bestimmter Funktionen des Produkts sind möglicherweise in der Trend Micro Online-Hilfe und/oder der Trend Micro Knowledge Base auf der Website von Trend Micro verfügbar.

Das Trend Micro Team ist stets bemüht, die Dokumentation zu verbessern. Bei Fragen, Anmerkungen oder Anregungen zu diesem oder anderen Dokumenten von Trend Micro wenden Sie sich bitte an docs@trendmicro.com.

Bewerten Sie diese Dokumentation auf der folgenden Website:

http://www.trendmicro.com/download/documentation/rating.asp



Inhaltsverzeichnis

Vorwort

Kapitel 1: Einführung in Endpoint Encryption

Kapitel 2: Systemvoraussetzungen

Kapitel 3: Übersicht über Verteilung und Upgrade

Kapitel 4: PolicyServer Verteilung

Kapitel 5: Integration des Control Managers

Kapitel 6: Verteilung von Endpoint Encryption Agents

Kapitel 7: Integration von OfficeScan

Kapitel 8: Wartung und technischer Support

Anhänge

Anhang A: Einführung in Trend Micro Control Manager

Anhang B: Überlegungen zur Verteilung

Anhang C: Pilotverteilung von Endpoint Encryption

Anhang D: Endpoint Encryption Dienste

Anhang E: Glossar

Stichwortverzeichnis



Vorwort

Vorwort

Willkommen beim Installations- und Migrationshandbuch für Trend Micro™ Endpoint Encryption™. Dieses Dokument enthält eine Einführung in die Sicherheitsarchitektur und die Funktionen von Endpoint Encryption, um Ihnen die Installation und Einrichtung in kürzester Zeit zu ermöglichen. In diesem Handbuch werden die Systemvoraussetzungen beschrieben, welche vorbereitenden Schritte für die Verteilung erforderlich sind und wie die Software für PolicyServer und Endpoint Encryption Agents installiert wird. Ferner wird beschrieben, wie Sie die Verteilung den Endbenutzern mitteilen und Upgrades und Migrationen durchführen.

Es werden folgende Themen behandelt:

Dokumente

In der Dokumentation zu Trend Micro Endpoint Encryption sind folgende Dokumente enthalten:

TABELLE 1. Produktdokumentation

DOKUMENT	BESCHREIBUNG
Administratorhandbuch	Enthält eine Beschreibung der Konzepte und Funktionen des Produkts sowie detaillierte Anweisungen zur Konfiguration und Verwaltung von PolicyServer, Full Disk Encryption und File Encryption.
Installations- und Migrationshandbuch	Enthält Erklärungen zu den Systemvoraussetzungen und detaillierte Anweisungen zur Verteilung, Installation, Migration und Aktualisierung von PolicyServer, Full Disk Encryption und File Encryption.
Online-Hilfe	Alle Produkte enthalten eine Möglichkeit zum Zugriff auf die Online-Hilfe. Die Online-Hilfe bietet Zugang zu kontextsensitiven HTML-Hilfethemen.
Readme-Datei	Enthält aktuelle Produktinformationen, die in der Online-Hilfe oder im Benutzerhandbuch noch nicht erwähnt sind. Zu den Themen gehören die Beschreibung neuer Funktionen, Lösungen bekannter Probleme und eine Liste bereits veröffentlichter Produktversionen.
Support-Portal	Eine Online-Datenbank mit Informationen zur Problemlösung und Fehlerbehebung. Sie enthält aktuelle Hinweise zu bekannten Softwareproblemen. Die Knowledge Base finden Sie im Internet unter folgender Adresse: http://esupport.trendmicro.com

Zielgruppe

Dieses Handbuch wurde für IT-Administratoren geschrieben, die Trend Micro Endpoint Encryption in mittleren bis großen Unternehmen einsetzen. Es richtet sich zudem an Helpdesk-Mitarbeiter, die Benutzer, Gruppen, Richtlinien und Geräte

verwalten. In dieser Dokumentation werden grundlegende Kenntnisse zu Geräten, Netzwerken und Sicherheit vorausgesetzt. Dazu gehören:

- Setup und Konfiguration der Endpunkt-Hardware
- Grundlegende Konzepte für die Endpunktverschlüsselung
- Partitionierung, Formatierung und Wartung der Festplatte
- Client-Server-Architektur

Dokumentationskonventionen

In der Dokumentation werden die folgenden Konventionen verwendet:

TABELLE 2. Dokumentationskonventionen

KONVENTION	BESCHREIBUNG
GROSSSCHREIBUNG	Akronyme, Abkürzungen und die Namen bestimmter Befehle sowie Tasten auf der Tastatur
Fettdruck	Menüs und Menübefehle, Schaltflächen, Registerkarten und Optionen
Kursivdruck	Referenzen auf andere Dokumente
`Schreibmaschinenschrift`	Beispiele für Befehlszeilen, Programmcode, Internet-Adressen, Dateinamen und Programmanzeigen
Navigationspfad >	Navigationspfad für den Zugriff auf ein bestimmtes Fenster Beispiel: **Datei** > **Speichern** bedeutet, auf der Benutzeroberfläche auf **Datei** und dann auf **Speichern** zu klicken
Hinweis	Konfigurationshinweise

KONVENTION	BESCHREIBUNG
Tipp	Empfehlungen oder Vorschläge
Wichtig	Informationen zu erforderlichen oder standardmäßigen Konfigurationseinstellungen und Produkteinschränkungen
Warnung!	Kritische Aktionen und Konfigurationsoptionen

Info über Trend Micro

Trend Micro, weltweit führend in der Internet-Content-Security und der Bewältigung von Bedrohungen, hat sich als Ziel gesetzt, den globalen Austausch von digitalen Informationen für Unternehmen und Endverbraucher sicher zu machen. Mit einer Erfahrung von über 20 Jahren bietet Trend Micro Client-, Server- und Cloud-basierte Lösungen, die neue Bedrohungen schneller unterbinden und die Daten in physischen, virtuellen und Cloud-Umgebungen schützen.

Da neue Bedrohungen und Schwachstellen immer wieder auftauchen, bleibt Trend Micro seiner Verpflichtung treu, seine Kunden beim Sichern von Daten, Einhalten der Konformität, Senken der Kosten und Wahren der Geschäftsintegrität zu unterstützen. Weitere Informationen finden Sie unter:

http://www.trendmicro.com

Trend Micro und das Trend Micro T-Ball-Logo sind Marken von Trend Micro Incorporated und in einigen Rechtsgebieten eingetragen. Alle anderen Marken- und Produktnamen sind Marken oder eingetragene Marken der entsprechenden Unternehmen.



Kapitel 1

Einführung in Endpoint Encryption

Dieses Kapitel besteht aus einer Einführung in die Funktionen, Merkmale, Geräte und Benutzer von Endpoint Encryption.

Es werden folgende Themen behandelt:

Info über Trend Micro Endpoint Encryption

Trend Micro Endpoint Encryption ist ein Garant für den Datenschutz, indem auf Endpunkten gespeicherte Daten, Dateien und Ordner sowie Wechselmedien auf vielen verschiedenen Plattformen verschlüsselt werden. Endpoint Encryption bietet eine granuläre Steuerung von Richtlinien und lässt sich flexibel in andere Verwaltungstools von Trend Micro integrieren, einschließlich Control Manager und OfficeScan. Die innovativen Verteilungsfunktionen unterstützen Sie dabei, Agent-Software ohne großen Aufwand mit FIPS 140-2-konformer Hardware-basierter oder Software-basierter Verschlüsselung zu verteilen, die für Endbenutzer völlig transparent ist und die Produktivität nicht beeinträchtigt. Nach der Verteilung wird die Sicherheitsverwaltung für Endpunkte durch automatisierte Berichterstellung, Audits und Richtliniensynchronisierung mit Endpoint Encryption PolicyServer vereinfacht.

Endpoint Encryption unterstützt Funktionen, um Remote-Befehle zu verteilen, verlorene Daten wiederherzustellen und die Identität der Benutzer zu schützen, während die Richtliniensynchronisierung in Echtzeit beibehalten wird. Wenn ein Endpunkt verloren geht oder gestohlen wird, können Sie von einem entfernten Standort aus einen Befehl zum Zurücksetzen oder „Auslöschen“ geben, um unverzüglich die unternehmensinternen Informationen zu schützen. Es gibt ebenfalls viele Wiederherstellungstools, die Endbenutzer bei der Datenrettung in dem Fall unterstützen, dass die Festplatte beschädigt wird. Endpoint Encryption fügt sich nahtlos in die vorhandenen unternehmensinternen Kontrollfunktionen ein und unterstützt eine Vielzahl von Authentifizierungsmethoden, einschließlich der Integration in Active Directory und Ressourcen für Endbenutzer, die ihre Anmeldedaten vergessen haben.

Wichtigste Funktionen und Vorteile

In der folgenden Tabelle werden die Hauptfunktionen und Vorteile von Endpoint Encryption erklärt.

Tabelle 1-1. Wichtigste Funktionen in Endpoint Encryption

Funktion	Vorteile
Verschlüsselung	• Schutz durch Full Disk Encryption, einschließlich MBR (Master Boot Record), Betriebssystem und alle Systemdateien • Hardware- und Software-basierte Verschlüsselung für gemischte Umgebungen • Umfassender Schutz von Dateien, Ordnern und Wechselmedien
Authentifizierung	• Flexible Authentifizierungsmethoden, einschließlich Einzel- und Multi-Faktor-Authentifizierung • Steuern der Kennwortstärke und Regelmäßigkeit von Kennwortänderungen • Richtlinienaktualisierungen vor der Authentifizierung und dem Systemstart • Konfigurierbare Aktionen für den Schwellenwert für die Eingabe falscher Kennwörter
Geräteverwaltung	• Richtlinien zum Schutz von Daten auf Endpunkten und Wechselmedien • Möglichkeit zum Sperren, Zurücksetzen, Löschen oder Auslöschen eines Geräts

FUNKTION	VORTEILE
Zentrale Verwaltung	• Flexible Verwendung entweder von PolicyServer MMC oder Control Manager zur Verwaltung von PolicyServer • Verteilung von Endpoint Encryption Agents auf Endpunkte, die bereits von OfficeScan verwaltet werden • Durchsetzung von Sicherheitsrichtlinien für Einzelpersonen oder Richtliniengruppen von einem einzigen Richtlinienserver aus • Unmittelbarer Schutz von Endbenutzerdaten durch Senden von Sperr- oder Löschbefehlen an verlorene oder gestohlene Endpoint Encryption Geräte • Automatisierte Durchsetzung von Richtlinien mit Korrekturen an Sicherheitsereignissen • Aktualisieren von Sicherheitsrichtlinien in Echtzeit vor der Authentifizierung, um Benutzer-Anmeldedaten vor dem Booten des Betriebssystems zu widerrufen
Aufzeichnung von Protokollen, Berichten und Auditing	• Erweiterte Berichtsfunktion und erweitertes Auditing in Echtzeit zur Einhaltung der Sicherheitsrichtlinien • Analysieren von Nutzungsstatistik mit geplanten Berichten und Warnmeldungen

Was ist neu in Version 5.0 Patch 1

Trend Micro Endpoint Encryption 5.0 Patch 1 umfasst viele neue Funktionen und Verbesserungen.

TABELLE 1-2. Was ist neu in Endpoint Encryption 5.0 Patch 1

NEUE FUNKTION	BESCHREIBUNG
Control Manager Lizenzverwaltung	Endpoint Encryption PolicyServer ist in die Lizenzverwaltung von Control Manager integriert. Control Manager unterstützt die folgenden Funktionen mit Endpoint Encryption: • Anzeigen der aktuellen Lizenzdaten von Endpoint Encryption • Verteilen einer Lizenz für eine Vollversion auf PolicyServer • Erneuern einer Lizenz in PolicyServer
Control Manager User-Centered Visibility	Endpoint Encryption ist in Control Manager User-Centered Visibility integriert. Die an Control Manager gesendeten Statusprotokolle enthalten Benutzerinformationen für die folgenden Endpoint Encryption Agents: • Full Disk Encryption • File Encryption • Encryption Management for Microsoft BitLocker • Encryption Management for Apple FileVault
Unterstützung für Netzwerkkarten und WLAN-Adapter	Endpoint Encryption unterstützt die folgenden Gruppen von Netzwerkkarten: • Intel Ethernet Controller I217 • Intel Ethernet Controller I218 Endpoint Encryption unterstützt ebenfalls den Intel Dual Band AC 7260 WLAN-Adapter.

TABELLE 1-3. Was ist neu in Endpoint Encryption 5.0

NEUE FUNKTION	BESCHREIBUNG
Neue Kommunikationsschnittstelle	In Endpoint Encryption 5.0 wurde eine neue Kommunikationsschnittstelle (Endpoint Encryption Dienst) eingeführt, über die alle Endpoint Encryption 5.0 Patch 1 Agents und Management-Konsolen mit PolicyServer kommunizieren. Der Endpoint Encryption Dienst verwendet eine Representational State Transfer Web-API (RESTful) mit einem AES-GCM-Verschlüsselungsalgorithmus. Der Endpoint Encryption Dienst hat drei Hauptfunktionen: • Zugriffssteuerung: Nach der Benutzerauthentifizierung generiert PolicyServer ein Token für den betreffenden Benutzer, das nur für diese Sitzung gültig ist. • Richtliniensteuerung: Vor der Benutzerauthentifizierung beschränkt der Endpoint Encryption Dienst alle Transaktionen von PolicyServer MMC, Control Manager und OfficeScan bis nach der Benutzerauthentifizierung. • Automatische Richtlinien-Updates: Nach der Registrierung bei PolicyServer rufen die Endpoint Encryption Agents automatisch neue Richtlinien ohne Benutzerauthentifizierung ab.
Integration des Control Managers	Endpoint Encryption 5.0 ist in Control Manager zur Verwaltung von PolicyServer integriert. Informationen zu Control Manager finden Sie unter *Info über Integration des Control Managers auf Seite 5-2*.
Integration von OfficeScan	Endpoint Encryption 5.0 unterstützt OfficeScan Installationen. Mit dem neuen Plug-in für das Endpoint Encryption Verteilungstool können Sie Endpoint Encryption Agents auf einen beliebigen Endpunkt verteilen, der momentan von OfficeScan verwaltet wird, oder vom betreffenden Endpunkt deinstallieren.

NEUE FUNKTION	BESCHREIBUNG
Lizenzverwaltung	Endpoint Encryption 5.0 ist in das Trend Micro Lizenzierungsportal integriert. Wie bei früheren Produktversionen können Sie Endpoint Encryption 30 Tage lang kostenlos ausprobieren. Nach Ablauf der Testlizenz ist ein Aktivierungscode erforderlich. Weitere Informationen zur Lizenzierung finden Sie unter *Wartungsvertrag auf Seite 8-2*.
Support für Apple FileVault™ und Microsoft BitLocker™	Endpoint Encryption 5.0 erweitert den Funktionsbereich von Full Disk Encryption, indem eine Integration mit Verschlüsselungslösungen, die zum Host-Betriebssystem gehören, durch zwei neue Endpoint Encryption Agents möglich gemacht wird: • Encryption Management for Microsoft BitLocker • Encryption Management for Apple FileVault Beide Agents werden zentral von PolicyServer über Richtlinien verwaltet, die bestimmen, ob das Endpoint Encryption Gerät von einem Remote-Standort aus gelöscht oder ausgelöscht werden soll.
Namensänderung von FileArmor und Wechsel zum Common Framework	Endpoint Encryption 5.0 benennt den FileArmor Agent in File Encryption um. Diese Änderung entspricht der neuen Funktionalität von Endpoint Encryption Agent besser. File Encryption verfügt über die Vorteile von FileArmor 3.1.3, einschließlich einer verbesserten Unterstützung für Wechselmedien. File Encryption wurde ebenfalls besser an Full Disk Encryption angepasst und unterstützt die verbesserte Kennwort- und Richtlinienverwaltung.

<table>
<tr><th>NEUE FUNKTION</th><th>BESCHREIBUNG</th></tr>
<tr><td>Verbesserungen bei Wartung, Protokollen und Berichten</td><td>Endpoint Encryption 5.0 zeichnet sich durch mehrere Verbesserungen in Bezug auf die Produktwartung, die Protokolle und die Berichte aus. Weitere Informationen finden Sie unter Erweiterte Funktionen für Unternehmen im Endpoint Encryption Administratorhandbuch.
Verfahren zum endgültigen Löschen der Protokolldatenbank: Es ist nun möglich, die Protokolldatenbank auf Grundlage spezifischer Kriterien endgültig zu löschen.
Inaktive Endpoint Encryption Benutzer und Geräte löschen: Um Geräte und Benutzer im Unternehmen zu bereinigen, ist es nun möglich, Geräte und Benutzer endgültig zu löschen, die seit einer bestimmten Zeit inaktiv sind.
Unternehmensbericht zu inaktiven Benutzern: Im neuen Unternehmensbericht werden alle Endpoint Encryption Benutzer aufgeführt, die sich seit einer bestimmten Zeit nicht bei einem Endpoint Encryption Gerät angemeldet haben.
Unternehmensbericht zu inaktiven Geräten: Im neuen Unternehmensbericht werden alle Endpoint Encryption Geräte aufgeführt, bei denen sich seit einer bestimmten Zeit kein Endpoint Encryption Benutzer mehr angemeldet hat.</td></tr>
<tr><td>Smartcard-Verbesserungen</td><td>Endpoint Encryption 5.0 unterstützt die folgenden Smartcard-Verbesserungen:
Verbesserte Verteilung von Endpoint Encryption Agents in Umgebungen, in denen Smartcards verwendet werden
Unterstützung für gemeinsame Smartcard-Kennwörter</td></tr>
</table>

Info über Verschlüsselung

Verschlüsselung bezeichnet den Vorgang, mit dem Daten unlesbar gemacht werden, wenn kein Zugriff auf den zur Verschlüsselung verwendeten Schlüssel besteht. Sie können die Verschlüsselung durch eine Software- oder Hardware-basierte Verschlüsselung (oder eine Kombination aus beidem) vornehmen, um Daten zu schützen, die sich lokal auf einer Endpunkt-Festplatte, auf einem Wechselmedium oder in bestimmten Dateien und Ordnern befinden und die in Netzwerken oder im Internet übertragen werden. Die Endpunktverschlüsselung ist das wichtigste Mittel, um die Datensicherheit zu gewährleisten und die Einhaltung gesetzlicher Vorschriften zum Datenschutz sicherzustellen.

Info über FIPS

Die *Federal Information Processing Standard (FIPS) Publication 140-2* ist ein Gerätesicherheitsstandard der US-amerikanischen Regierung, der die Sicherheitsstandards für Verschlüsselungsmodule vorgibt. In der folgenden Tabelle werden die vier Stufen der FIPS 140-2-Sicherheit erklärt:

Tabelle 1-4. FIPS 140-2-Sicherheitsstufen

Stufe	Beschreibung
1	Alle Verschlüsselungskomponenten müssen sich auf der Produktionsstufe befinden und dürfen keine Sicherheitslücken aufweisen.
2	Beinhaltet alle Anforderungen von Stufe 1 und fügt physischen Manipulationsbeweis und rollenbasierte Authentifizierung hinzu.
3	Beinhaltet alle Anforderungen von Stufe 2 und fügt physischen Manipulationswiderstand und identitätsbasierte Authentifizierung hinzu.
4	Beinhaltet alle Anforderungen von Stufe 3 und fügt weitere physische Sicherheitsanforderungen hinzu.

Komponenten von Endpoint Encryption

Endpoint Encryption besteht aus einem zentralen Verwaltungsserver (PolicyServer), der die Richtlinien- und Protokolldatenbanken, die Authentifizierung und alle Client-Server-Aktivitäten verwaltet. Sie können mehrere eindeutige Endpoint Encryption Agents verteilen, die jeweils spezifische Verschlüsselungsaufgaben ausführen. Alle Endpoint Encryption Agents kommunizieren über einen verschlüsselten Kanal.

Sie können Endpoint Encryption nur mit PolicyServer MMC flexibel verwalten, oder Sie verwalten Endpoint Encryption mit Control Manager für die Verwaltung von Richtlinien, Benutzern und Geräten und setzen PolicyServer MMC für die erweiterte Protokollverwaltung und Berichterstellung ein.

Endpoint Encryption und OfficeScan können integriert werden. Mit dem Plug-in für das Endpoint Encryption Verteilungstool können Sie die Software des Endpoint Encryption Agent auf beliebige verwaltete OfficeScan Endpunkte verteilen.



Hinweis

Informationen zu Verteilungsszenarien finden Sie unter *Übersicht über Verteilung und Upgrade auf Seite 3-1*.

In der folgenden Darstellung werden die Komponenten und Kommunikationsprotokolle von Endpoint Encryption illustriert.

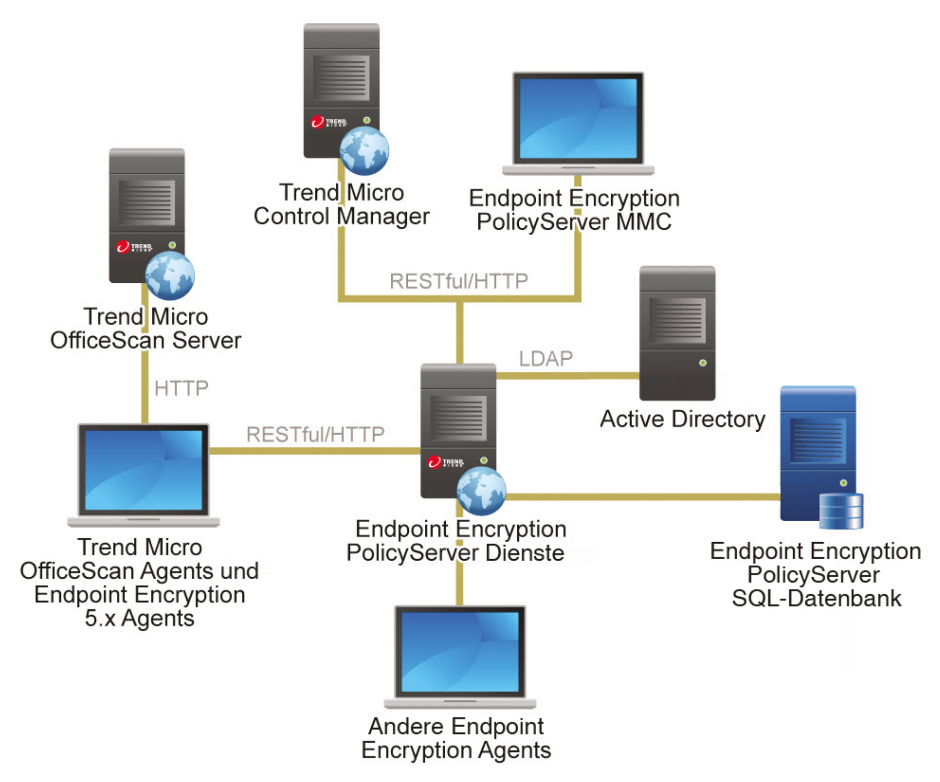


ABBILDUNG 1-1. Architektur von Endpoint Encryption

In der folgenden Tabelle werden diese Komponenten beschrieben.

TABELLE 1-5. Komponenten von Endpoint Encryption

KOMPONENTE	BESCHREIBUNG
Endpoint Encryption PolicyServer Dienste	PolicyServer besteht aus mehreren Diensten, die Richtlinien, Authentifizierung und Berichterstellung zentral steuern. PolicyServer besteht aus den folgenden Elementen: • Endpoint Encryption Dienst • Legacy Web-Service • PolicyServer Windows-Dienst Weitere Informationen zu PolicyServer finden Sie unter *Info über PolicyServer auf Seite 1-13*.
Endpoint Encryption PolicyServer SQL-Datenbank	In der Microsoft™ SQL Server-Datenbank werden alle Informationen zu Benutzern, Richtlinien und Protokollen gespeichert. Sie können die Datenbank auf demselben Server wie PolicyServer oder getrennt davon installieren. Sie können PolicyServer flexibel mit Microsoft SQL Server oder Microsoft SQL Express konfigurieren. Informationen zu den Optionen zur Datenbankkonfiguration finden Sie unter *Empfehlungen zur Skalierung auf Seite 3-18*.
Endpoint Encryption PolicyServer MMC	PolicyServer MMC ist die native Schnittstellenoption, um PolicyServer von einem Remote-Standort aus zu verwalten.
Trend Micro Control Manager	Trend Micro Control Manager ist eine Option, um PolicyServer von einem Remote-Standort aus zu verwalten, wobei die Lösung ebenfalls eine Integration mit anderen verwalteten Produkten von Trend Micro bereitstellt. Administratoren können mit den Funktionen zur Richtlinienverwaltung die Produkteinstellungen für die verwalteten Produkte und Endpunkte konfigurieren und verteilen. Die webbasierte Management-Konsole von Control Manager bietet einen zentralen Überwachungspunkt für die Verwaltung der Produkte und Dienste für Virenschutz und Content Security im gesamten Netzwerk.

Komponente	Beschreibung
Endpoint Encryption 5.0 Patch 1 agents	Alle Endpoint Encryption 5.0 Patch 1 Agents kommunizieren mit dem PolicyServer Endpoint Encryption Dienst unter Verwendung einer Web-API (RESTful). Weitere Informationen zu den Endpoint Encryption Agents finden Sie unter: • *Info über Full Disk Encryption auf Seite 6-3* • *Info über die File Encryption auf Seite 6-4* Informationen zur Kommunikation von Endpoint Encryption Agents finden Sie unter *Info über PolicyServer auf Seite 1-13*. **Hinweis** Sie können die Porteinstellungen während der Installation von Endpoint Encryption konfigurieren. Mit der Full Disk Encryption Wiederherstellungskonsole können Sie die zugewiesene Portnummer ändern.
Andere Endpoint Encryption Agents	Alle älteren Endpoint Encryption Agents (3.1.3 und älter) kommunizieren mit dem Legacy Web Service auf PolicyServer. Detaillierte Hinweise zur Kommunikation mit Agents finden Sie unter *Info über PolicyServer auf Seite 1-13*.
Active Directory	PolicyServer synchronisiert Benutzerkontoinformationen durch Kommunikation mit Active Directory über LDAP. Die Kontoinformationen werden in der Microsoft SQL-Datenbank zwischengespeichert. **Hinweis** Active Directory ist optional.

Info über PolicyServer

Trend Micro PolicyServer verwaltet Verschlüsselungsschlüssel und synchronisiert Richtlinien mit allen Endpunkten im Unternehmen. PolicyServer setzt ferner die sichere

Authentifizierung durch und umfasst Echtzeit-Audits und Tools zur Berichterstellung, um die Einhaltung von gesetzlichen Bestimmungen sicherzustellen. Sie können PolicyServer with PolicyServer MMC oder mit Trend Micro Control Manager flexibel verwalten. Andere Funktionen zur Datenverwaltung umfassen benutzerseitige Selbsthilfe-Optionen und Geräteaktionen, um ein verlorenes oder gestohlenes Gerät von einem entfernten Standort aus zurückzusetzen oder „auszulöschen".

In der folgenden Tabelle werden die Komponenten von PolicyServer beschrieben, die Sie abhängig von den Anforderungen in der Umgebung auf einem oder mehreren Servern verteilen können.

TABELLE 1-6. Komponenten von PolicyServer

KOMPONENTE	BESCHREIBUNG
Unternehmen	"Endpoint Encryption - Unternehmen" ist der eindeutige Bezeichner für das Unternehmen in der PolicyServer Datenbank, der bei der Installation von PolicyServer konfiguriert wurde. In einer PolicyServer Datenbank darf es nur eine Unternehmenskonfiguration geben.
Datenbank	In der Microsoft SQL-Datenbank von PolicyServer werden alle Benutzer, Geräte und Protokolldaten sicher gespeichert. Die Datenbank ist entweder auf einem dedizierten Server konfiguriert oder wird einem vorhandenen SQL-Cluster hinzugefügt. Die Protokoll- und anderen Datenbanken können sich an unterschiedlichen Speicherorten befinden.
PolicyServer Windows-Dienst	Der PolicyServer Windows-Dienst verwaltet alle Kommunikationstransaktionen zwischen Host-Betriebssystem, Endpoint Encryption Dienst, Legacy Web-Service, Client Web Proxy und SQL-Datenbanken.

KOMPONENTE	BESCHREIBUNG
Endpoint Encryption Dienst	Alle Endpoint Encryption 5.0 Patch 1 Agents nutzen den Endpoint Encryption Dienst zur Kommunikation mit PolicyServer. Der Endpoint Encryption Dienst verwendet eine Representational State Transfer Web-API (RESTful) mit einem AES-GCM-Verschlüsselungsalgorithmus. Nachdem sich ein Benutzer authentifiziert hat, generiert PolicyServer ein Token im Zusammenhang mit der spezifischen Richtlinienkonfiguration. Bis zur Authentifizierung durch den Endpoint Encryption Benutzer sperrt der Dienst alle Richtlinientransaktionen. Um eine dreistufige Netzwerktopographie zu erstellen, kann der Dienst auch gesondert auf einen Endpunkt verteilt werden, der sich in der Netzwerk-DMZ befindet. Dadurch kann sich PolicyServer sicher hinter der Firewall befinden.
Legacy Web-Service	Alle Agents von Endpoint Encryption 3.1.3 und niedriger verwenden das Simple Object Access Protocol (SOAP), um mit PolicyServer zu kommunizieren. In bestimmten Situationen erlaubt SOAP möglicherweise unsichere Richtlinientransaktionen ohne Benutzerauthentifizierung. Legacy Web Service filtert SOAP-Aufrufe, indem eine Authentifizierung erforderlich gemacht wird und die Befehle begrenzt werden, die SOAP akzeptiert. Um eine dreistufige Netzwerktopographie zu erstellen, kann der Dienst auch gesondert auf einen Endpunkt verteilt werden, der sich in der Netzwerk-DMZ befindet. Dadurch kann sich PolicyServer sicher hinter der Firewall befinden.

Management-Konsolen

Abhängig von den Anforderungen an die Endpunktsicherheit und die vorhandene Infrastruktur können Sie Endpoint Encryption nur mit einer Management-Konsole oder einer Kombination aus mehreren Management-Konsolen verwalten. In der folgenden Tabelle werden die verfügbaren Management-Konsolen zum Verwalten von Endpoint Encryption beschrieben.

TABELLE 1-7. Endpoint Encryption Management-Konsolen

MANAGEMENT-KONSOLE	BESCHREIBUNG
PolicyServer MMC	Das Plug-in PolicyServer Microsoft Management Console (PolicyServer MMC) ist die native Management-Konsole zur Verwaltung von Richtlinien, Benutzern und Geräten für Endpoint Encryption. Sie können mit PolicyServer MMC Folgendes zentral verwalten: • Alle Benutzer, Geräte und Gruppen von Endpoint Encryption • Alle Verschlüsselungs-, Kennwortkomplexitäts- und Authentifizierungsrichtlinien • Remote-Aktionen zur Gerätemanipulation, inkl. Auslöschen eines Geräts, Löschen von Daten oder Verzögern der Authentifizierung • Ereignisprotokolle über Authentifizierungsereignisse, Verwaltungsereignisse und Sicherheitsverstöße sowie den Geräteverschlüsselungsstatus • Remote-Hilfe zum Zurücksetzen des Kennworts • Optionen für Audits und Berichterstellung

Management-Konsole	Beschreibung
Control Manager	Der Trend Micro Control Manager ist eine zentrale Management-Konsole zur Verwaltung von Produkten und Services von Trend Micro auf Gateways, Mail-Servern, File-Servern und Unternehmensdesktops. Administratoren können mit den Funktionen zur Richtlinienverwaltung die Produkteinstellungen für die verwalteten Produkte und Endpunkte konfigurieren und verteilen. Die webbasierte Management-Konsole von Control Manager bietet einen zentralen Überwachungspunkt für die Verwaltung der Produkte und Dienste für Virenschutz und Content Security im gesamten Netzwerk. Sie können eine mehrschichtige Sicherheit schaffen, indem Sie Endpoint Encryption mit Control Manager als verwaltetes Trend Micro Produkt integrieren. Sie können Endpoint Encryption nur mit PolicyServer MMC flexibel verwalten, oder Sie verwalten Endpoint Encryption mit Control Manager für die Verwaltung von Richtlinien, Benutzern und Geräten und setzen PolicyServer MMC für die erweiterte Protokollverwaltung und Berichterstellung ein.
OfficeScan	OfficeScan schützt Unternehmensnetzwerke vor Malware, Netzwerkviren, webbasierten Bedrohungen, Spyware und kombinierten Bedrohungen. OfficeScan ist eine integrierte Lösung und besteht aus einem Agent am Endpunkt sowie einem Serverprogramm, das alle Agents verwaltet. Mit dem OfficeScan Plug-in für das Endpoint Encryption Verteilungstool können Sie Endpoint Encryption Agents auf einen beliebigen Endpunkt verteilen, der momentan von OfficeScan verwaltet wird, oder vom betreffenden Endpunkt deinstallieren.

Endpoint Encryption Agents

In der folgenden Tabelle werden die Endpoint Encryption Agents beschrieben, die für eine Vielzahl von Umgebungen verfügbar sind.

AGENT	BESCHREIBUNG
File Encryption	Der Endpoint Encryption Agent für die Verschlüsselung von Dateien und Ordnern auf lokalen Laufwerken und Wechselmedien. Mit File Encryption können Sie die Dateien und Ordner auf nahezu jedem Gerät, das als Laufwerk im Host-Betriebssystem angezeigt wird, schützen. Weitere Informationen finden Sie unter *Info über die File Encryption auf Seite 6-4*.
Full Disk Encryption	Der Endpoint Encryption Agent für die Verschlüsselung von Hardware und Software mit Preboot-Authentifizierung. Sie können mit Full Disk Encryption Datendateien, Anwendungen, Registrierungseinstellungen, temporäre Dateien, Auslagerungsdateien, Druck-Spooler und gelöschten Dateien auf allen Windows-Endpunkten sichern. Eine starke Preboot-Authentifizierung beschränkt den Zugriff auf das anfällige Systeme, bis der Benutzer validiert wird. Weitere Informationen finden Sie unter *Info über Full Disk Encryption auf Seite 6-3*.
Encryption Management for Microsoft BitLocker	Der Endpoint Encryption Full Disk Encryption Agent für Microsoft Windows-Umgebungen, auf denen lediglich Microsoft BitLocker auf dem Hosting-Endpunkt aktiviert werden muss. Mit dem Encryption Management for Microsoft BitLocker Agent können Sie Endpunkte mit Trend Micro Full Disk Encryption in einer bestehenden Windows-Infrastruktur sichern. Weitere Informationen finden Sie unter *Info über Full Disk Encryption auf Seite 6-3*.

AGENT	BESCHREIBUNG
Encryption Management for Apple FileVault	Der Endpoint Encryption Full Disk Encryption Agent für Mac OS-Umgebungen, auf denen lediglich Apple FileVault auf dem Hosting-Endpunkt aktiviert werden muss. Mit der Encryption Management for Apple FileVault Agent können Sie Endpunkte mit Trend Micro Full Disk Encryption in einer bestehenden Mac OS-Infrastruktur sichern. Weitere Informationen finden Sie unter *Info über Full Disk Encryption auf Seite 6-3*.



Hinweis

Endpoint Encryption 5.0 verfügt über keine KeyArmor Geräte. Es werden jedoch ältere KeyArmor Geräte unterstützt.

Endpoint Encryption - Geräte

Endpoint Encryption Geräte sind Endpoint Encryption Agents, die bei PolicyServer registriert wurden. Bei der Installation eines Endpoint Encryption Agent wird der Endpunkt automatisch bei PolicyServer als ein Endpoint Encryption Gerät registriert. Da ein bestimmter Endpunkt von mehreren Endpoint Encryption Agents geschützt werden kann, erscheint ein einzelner Endpunkt möglicherweise als mehrere Endpoint Encryption Geräte auf PolicyServer.

Sie können Richtlinienregeln festlegen, die automatisch nach zu vielen fehlgeschlagenen Authentifizierungsversuchen oder, wenn der Endpoint Encryption Agent veraltete Richtlinien hat, ausgelöst werden. Folgende Richtlinienregeln sind verfügbar:

- Zeitverzögerung
- Remote-Authentifizierung erforderlich
- Gerät löschen

PolicyServer kann unverzüglich bei verlorenen und gestohlenen Endpunkten aktiv werden, indem eine Remote-Aktion auf dem betreffenden Endpoint Encryption Gerät ausgeführt wird. Die folgenden Remote-Aktionen sind verfügbar:

- Software-Token
- Wiederherstellungsschlüssel
- Gerät auslöschen
- Gerät sperren
- Warmstart



Hinweis

Weitere Informationen über das Endpoint Encryption Gerät finden Sie unter *Geräte und Benutzer* im *Endpoint Encryption Administratorhandbuch*.

Endpoint Encryption Benutzer

Bei Endpoint Encryption Benutzern handelt es sich um alle Benutzerkonten, die manuell zum PolicyServer hinzugefügt oder die mit Active Directory synchronisiert wurden.

Endpoint Encryption verfügt über mehrere Typen von Kontorollen und Authentifizierungsmethoden, die eine umfassende, auf Identität basierende Authentifizierung und Verwaltung möglich machen. Mit Control Manager oder PolicyServer MMC können Sie Benutzerkonten hinzufügen oder importieren, die Authentifizierung steuern, mit Active Directory eine Synchronisierung durchführen und die Mitgliedschaft in Richtliniengruppen bei Bedarf verwalten.



Hinweis

Weitere Informationen über Endpoint Encryption Benutzer und Authentifizierung finden Sie unter *Geräte und Benutzer* im *Endpoint Encryption Administratorhandbuch*.

Endpoint Encryption Benutzerrollen

In der folgenden Tabelle werden die Endpoint Encryption Benutzerkontentypen beschrieben, die für die verschiedenen Rollen innerhalb des Unternehmens oder der Richtliniengruppe gedacht sind. Jede Rolle bestimmt die Berechtigungen, die gewährt

werden, wenn der Benutzer auf die Endpoint Encryption Management-Konsolen und Geräte zugreift.

TABELLE 1-8. Endpoint Encryption Kontenrollen

ROLLE	BESCHREIBUNG
Unternehmensadministrator	Gedacht für Administratoren, die Aufgaben auf Unternehmensebene ausführen, Diese Administratoren verfügen über administrative Rechte für alle Gruppen, Benutzer, Geräte und Richtlinien, unabhängig davon, wo sie sich innerhalb des Unternehmens befinden.
Gruppen- oder Richtlinienadministrator*	Gedacht für Administratoren, die Aufgaben in Bezug auf Gruppen oder Richtlinien ausführen. **Hinweis** Diese Berechtigungen gelten nicht für übergeordnete Gruppen, Gruppen auf derselben Hierarchieebene oder deren Untergruppen.
Unternehmensauthentifizierer	Gedacht für Helpdesk-Mitarbeiter, die Remote-Unterstützung für Benutzer anbieten, die ihr Endpoint Encryption Kennwort vergessen oder technische Probleme haben. Unternehmensauthentifizierer haben Berechtigungen, die für das Unternehmen konfiguriert werden können.
Gruppen- oder Richtlinienauthentifizierer*	Gedacht für Helpdesk-Mitarbeiter mit denselben Berechtigungen wie der Unternehmensauthentifizierer, mit der Ausnahme, dass diese Berechtigungen nur für die zugewiesene Gruppe oder Richtlinie gelten.
Benutzer	Gedacht für einfache Endbenutzer ohne spezielle Berechtigungen. Die Benutzerrolle kann sich nicht an Endpoint Encryption Management-Konsolen anmelden.



Hinweis

*Wegen der unterschiedlichen Richtlinienarchitektur führt Control Manager die Richtlinien- und Gruppenstruktur von PolicyServer MMC zusammen. Die folgenden Rollen sind in PolicyServer MMC und Control Manager identisch:

- Gruppenadministrator (PolicyServer MMC) und Richtlinienadministrator (Control Manager)
- Gruppenauthentifizierer (PolicyServer MMC) und Richtlinienauthentifizierer (Control Manager)



Kapitel 2

Systemvoraussetzungen

In diesem Kapitel werden die Systemvoraussetzungen für Trend Micro Endpoint Encryption beschrieben.

Es werden folgende Themen behandelt:

- *Voraussetzungen für PolicyServer auf Seite 2-2*
- *Management-Konsolen auf Seite 2-6*
- *Agents auf Seite 2-9*

Voraussetzungen für PolicyServer

In diesem Abschnitt werden die Hardware- und Software-Voraussetzungen für PolicyServer beschrieben, die zum Ausführen der Installationen erforderlichen Dateien sowie die zum Einrichten der Datenbank- und Windows-Server-Umgebungen benötigten Konten.

Systemvoraussetzungen für PolicyServer

TABELLE 2-1. Systemvoraussetzungen für PolicyServer

<table>
<tr><th>SPEZIFIKATION</th><th>VORAUSSETZUNGEN</th></tr>
<tr><td>Prozessor</td><td rowspan="3">Siehe Überlegungen zu Datenbanken auf Seite 2-4.</td></tr>
<tr><td>RAM</td></tr>
<tr><td>Festplattenspeicher</td></tr>
<tr><td>Betriebssystem</td><td>• Windows Server 2003 SP2 32 Bit/64 Bit
• Windows Server 2008 / 2008 R2 64 Bit

Hinweis
Weitere Informationen zu den Voraussetzungen für Windows Server 2008 / 2008 R2 finden Sie unter Überlegungen zu Windows Server 2008 und 2008 R2 auf Seite 2-3.</td></tr>
<tr><td>Datenbank</td><td>• Microsoft SQL 2005 SP3 (32 Bit/64 Bit) / 2008 / 2008 R2
• Microsoft SQL Express 2005 SP3 / 2008
• Mixed Mode Authentication (SA-Kennwort) installiert
• Berichtsdienste installiert</td></tr>
</table>

SPEZIFIKATION	VORAUSSETZUNGEN
Webserver und andere Software	• Anwendungsserver • Microsoft IIS **Hinweis** PolicyServer 5.0 Patch 1 erfordert einen IIS-Standort. Wenn Client-Web-Service auf einem Remote-Endpunkt verwendet wird, stellen Sie sicher, dass die Microsoft IIS-Dienste installiert werden. **Wichtig** Sorgen Sie dafür, dass in Windows 2003/2008 64-Bit-Umgebungen für die IIS-Einstellung „Enable32BitAppOnWin64“ "false" festgelegt wird. • ASP (Active Server Pages) zulassen • ASP.NET zulassen • Sowohl Microsoft .NET Framework 2.0 SP2 (oder 3.5) als auch 4.0 • Windows Installer 4.5 (SQL Express)

Überlegungen zu Windows Server 2008 und 2008 R2

In der folgenden Tabelle werden die zusätzlichen Voraussetzungen zur Installation von PolicyServer unter Microsoft Windows Server 2008 oder Microsoft Windows Server 2008 R2 beschrieben.

<table>
<tr><th>BETRIEBSSYSTEM</th><th>ROLLEN</th><th>FUNKTIONEN</th><th>ANDERE</th></tr>
<tr><td>2008</td><td rowspan="2">• Anwendungsserverrolle installieren
• Webserverrolle installieren</td><td rowspan="2">• SMTP hinzufügen
• Unterstützung für Microsoft IIS hinzufügen</td><td>• Microsoft .NET Framework 4.0 installieren</td></tr>
<tr><td>2008 R2</td><td>• Zum Ausführen von SQL 2008 muss SQL 2008 SP1 installiert werden
• Kein .NET-Upgrade erforderlich</td></tr>
</table>

Überlegungen zu Datenbanken

Für die Installation von PolicyServer wird empfohlen, dass mindestens zwei dedizierte Server zur Verfügung stehen:

1. Ein Server für die Datenbank. Alternativ können Sie die Datenbank zu einem vorhandenen SQL-Cluster hinzufügen.
2. Ein dedizierter Server für die PolicyServer Dienste.



Hinweis

Virtualisierte Hardware wird unter VMware Virtual Infrastructure unterstützt.

TABELLE 2-2. Hardware-Voraussetzungen für PolicyServer

SEPARATE HOSTS		EINZELNER HOST
PolicyServer Host (3.000 Benutzer)	SQL-Server-Host (3.000 Benutzer)	PolicyServer und SQL-Server (1.500 Benutzer)

SEPARATE HOSTS		EINZELNER HOST
• 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Prozessoren • 4GB Arbeitsspeicher • 40 GB Festplattenspeicher	• 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Prozessoren • 8GB Arbeitsspeicher • 100GB Festplattenspeicher	• 2 GHz Quad Core Core2 Intel™ Xeon™ Prozessoren • 8GB Arbeitsspeicher • 120GB Festplattenspeicher

Erforderliche Installationsdateien

Kopieren Sie vor der Installation alle Installationsdateien auf die lokale Festplatte.

TABELLE 2-3. Dateien, die für die Installation von PolicyServer benötigt werden

DATEI	ZWECK
`PolicyServerInstaller.exe`	Installiert PolicyServer Datenbanken und Dienste. Optional kann PolicyServer MMC gleichzeitig installiert werden.
`PolicyServerMMCSnapinSetup.msi`	Installiert nur PolicyServer MMC.
`TMEEProxyInstaller.exe`	Installiert den Client-Web-Service und den Traffic Forwarding Service. Diese Dienste fungieren als Web-Proxys und Kommunikationsprotokolle für Umgebungen, in denen sich PolicyServer und Endpoint Encryption Agents in unterschiedlichen LANs befinden. Client-Web-Service bietet Funktionen für ältere Agents und Traffic Forwarding Service für Agents der Versionen 5.0 oder höher.



Hinweis

PolicyServer enthält eine Testlizenz für 30 Tage. Eine Lizenzdatei ist nicht mehr erforderlich, um ein Upgrade auf die Vollversion durchzuführen. Weitere Informationen finden Sie unter *Wartung und technischer Support auf Seite 8-1*.

Erforderliche Konten

In der folgenden Tabelle werden die Konten beschrieben, die für PolicyServer erforderlich sind.

TABELLE 2-4. Konten, die für die Installation von PolicyServer benötigt werden

KONTO	FUNKTION	BESCHREIBUNG
SQL SA	PolicyServer Installationsprogramm	Das Konto wird nur zum Erstellen der PolicyServer Datenbanken verwendet.
SQL MADB	PolicyServer Windows-Dienst	Das Konto wird während der Installation zum Authentifizieren bei den PolicyServer Datenbanken erstellt.
Lokaler Administrator	PolicyServer Windows-Dienst und IIS	Über dieses Konto werden der PolicyServer Windows-Dienst und der Web-Service ausgeführt.

Management-Konsolen

In diesem Abschnitt werden die Voraussetzungen für Management-Konsolen beschrieben.

Systemvoraussetzungen für PolicyServer MMC

In der folgenden Tabelle werden die Systemvoraussetzungen für PolicyServer MMC beschrieben. Sie können es bei der Installation von PolicyServer oder separat auf einem anderen Endpunkt installieren.

TABELLE 2-5. Systemvoraussetzungen für PolicyServer MMC

SPEZIFIKATION	VORAUSSETZUNGEN
Prozessor	Intel™ Core™ 2 oder kompatibler Prozessor

Spezifikation	Voraussetzungen
RAM	512MB
Festplattenspeicher	Mindestens 100MB
Netzwerkverbindung	Verbindung mit PolicyServer
Betriebssystem	Jedes Microsoft Windows-Betriebssystem, das von PolicyServer oder den Endpoint Encryption Agents unterstützt wird
Andere	• Microsoft .NET Framework 4.0

Systemvoraussetzungen für Control Manager

In der folgenden Tabelle werden die Voraussetzungen beschrieben, die zum Verwenden von Control Manager zur Serververwaltung erfüllt werden müssen.

Tabelle 2-6. Voraussetzungen für Control Manager

Spezifikation	Voraussetzungen
Control Manager Server	Control Manager, Patch 3
RAM	• Mindestens 2GB • 4GB empfohlen
Festplattenspeicher	• Mindestens 10GB • 20GB empfohlen
Netzwerkverbindung	Verbindung mit PolicyServer
Andere	Angaben zu den weiteren Systemvoraussetzungen für Control Manager sowie die Setup-Anweisungen finden Sie in der Control Manager Dokumentation, die Sie unter folgender Adresse herunterladen können: http://docs.trendmicro.com/en-us/enterprise/control-manager.aspx

Systemvoraussetzungen für OfficeScan

In den folgenden Tabellen werden die Systemvoraussetzungen zur Installation von OfficeScan, zur Verwendung des Plug-in für das Endpoint Encryption Verteilungstool zur Verteilung von Endpoint Encryption Agents und zur Installation des OfficeScan Agent beschrieben.

TABELLE 2-7. OfficeScan Server Voraussetzungen

SPEZIFIKATION	VORAUSSETZUNGEN
OfficeScan Server	Eine der folgenden Versionen: • 10.6 SP3 • 10.5 Patch 5
Plug-in-Manager	2.0
RAM	• Mindestens 1 GB, wobei mindestens 500 MB für OfficeScan zur Verfügung stehen • 2GB empfohlen
Speicherplatz für OfficeScan	• Mindestens 3,1 GB, wenn sich auf dem Server Folgendes befindet: • OfficeScan server • OfficeScan Client • Policy Server für Cisco™ NAC • Integrierter Smart Protection Server (lokal) • Mindestens 3,5GB, wenn sich auf dem Server Folgendes befindet: • OfficeScan server • OfficeScan Client • Integrierter Smart Protection Server (remote)
Speicherplatz für Endpoint Encryption Verteilungstool	Mindestens 1GB

Spezifikation	Voraussetzungen
Netzwerkverbindung	• Verbindung mit PolicyServer • Verbindung mit OfficeScan Endpunkten
Andere	Angaben zu den weiteren Systemvoraussetzungen für OfficeScan sowie die Setup-Anweisungen finden Sie in der OfficeScan Dokumentation, die Sie unter folgender Adresse herunterladen können: http://docs.trendmicro.com/de-de/enterprise/officescan.aspx

Tabelle 2-8. Voraussetzungen für OfficeScan Agent

Spezifikation	Voraussetzungen
RAM	• Mindestens 512MB
Festplattenspeicher	• Mindestens 1GB
Netzwerkverbindung	• Verbindung mit PolicyServer • Verbindung mit OfficeScan Endpunkten
Andere	Microsoft .NET Framework 2.0 SP1 **Hinweis** Obwohl OfficeScan Agents unter allen Windows Versionen ausgeführt werden können, sollten Sie unbedingt die Systemvoraussetzungen für den jeweiligen Endpoint Encryption Agent lesen.

Agents

In diesem Abschnitt werden die Voraussetzungen für alle Endpoint Encryption Agents kurz beschrieben.

Full Disk Encryption Systemvoraussetzungen

In den folgenden Tabellen werden die minimalen und empfohlenen Systemanforderungen zur Installation von Full Disk Encryption beschrieben.

TABELLE 2-9. Full Disk Encryption Systemvoraussetzungen

SPEZIFIKATION	VORAUSSETZUNGEN
Prozessor	Intel™ Core™ 2 oder kompatibler Prozessor
RAM	Mindestens 1GB
Festplattenspeicher	• Mindestens 30GB • 20 % freier Speicherplatz erforderlich • 256MB zusammenhängender freier Speicher erforderlich
Netzwerkverbindung	Kommunikation mit PolicyServer für verwaltete Agents erforderlich
Betriebssystem	• Windows™ 8.1 (32 Bit/64 Bit) • Windows™ 8 (32 Bit/64 Bit) • Windows™ 7 (32 Bit/64 Bit) • Windows™ Vista mit SP1 (32 Bit/64 Bit) • Windows™ XP mit SP3 (nur 32 Bit)
Andere Software	Weitere Anforderungen für Windows 8: • Microsoft .NET Framework 3.5 aktiviert • Bei Geräten mit UEFI legen Sie die Startreihenfolge auf **Legacy First** fest. Weitere Informationen finden Sie unter *Windows-Endpunkt vorbereiten auf Seite 6-8*. Weitere Voraussetzungen für Windows XP: • Microsoft .NET Framework 2.0 SP1 oder höher • Microsoft Windows Installer 3.1

SPEZIFIKATION	VORAUSSETZUNGEN
Festplatte	• Seagate DriveTrust-Laufwerke • Seagate OPAL- und OPAL 2-Laufwerke **Hinweis** • Sie dürfen Full Disk Encryption nicht auf Endpunkte mit mehreren Festplatten installieren. Umgebungen mit mehreren Festplatten werden nicht unterstützt. • RAID- und SCSI-Festplatten werden nicht unterstützt. • Full Disk Encryption für Windows 8 unterstützt keine RAID-, SCSI- oder eDrive-Laufwerke.
Andere Hardware	• Software-Verschlüsselung: ATA-, AHCI- oder IRRT-Festplattencontroller **Hinweis** RAID- und SCSI-BIOS-Einstellungen werden nicht unterstützt. • Hardware-Verschlüsselung: AHCI-Festplattencontroller **Hinweis** Andere BIOS-Einstellungen werden nicht unterstützt.

Systemvoraussetzungen für die Encryption Management for Microsoft BitLocker

In der folgenden Tabelle werden die minimalen und empfohlenen Systemvoraussetzungen für die Encryption Management for Microsoft BitLocker beschrieben.

TABELLE 2-10. Systemvoraussetzungen für die Encryption Management for Microsoft BitLocker

SPEZIFIKATION	VORAUSSETZUNGEN
Prozessor	Intel™ Core™ 2 oder kompatibler Prozessor.
Arbeitsspeicher	Die Voraussetzungen basieren auf den Systemvoraussetzungen für Windows: • 64-Bit-Systeme: 2GB • 32-Bit-Systeme: 1GB
Festplattenspeicher	• Mindestens 30GB • 20 % freier Speicherplatz erforderlich • 100 MB zusammenhängender freier Speicher erforderlich
Festplatte	• Standardlaufwerke, die von Windows unterstützt werden
Netzwerkverbindung	Verbindung mit PolicyServer
Betriebssystem	• Windows™ 8.1 (32 Bit/64 Bit) Enterprise und Professional Editionen • Windows 8™ (32 Bit/64 Bit) Enterprise und Professional Editionen • Windows 7™ (32 Bit/64 Bit) Enterprise und Ultimate Editionen
Andere Software	• Trusted Platform Module (TPM) 1.2 oder höher • Full Disk Encryption ist nicht installiert • Windows BitLocker ist deaktiviert • Microsoft .NET Framework 3.5

Systemvoraussetzungen für die Encryption Management for Apple FileVault

In der folgenden Tabelle werden die minimalen und empfohlenen Systemvoraussetzungen für die Encryption Management for Apple FileVault beschrieben.

TABELLE 2-11. Systemvoraussetzungen für die Encryption Management for Apple FileVault

SPEZIFIKATION	VORAUSSETZUNG
Prozessor	Intel™ Core™ 2 oder kompatibler Prozessor
Arbeitsspeicher	• Mindestens 512MB • 1GB empfohlen
Festplattenspeicher	• Mindestens 400MB
Netzwerkverbindung	Verbindung mit PolicyServer
Betriebssystem	• Mac OS X Mavericks™ • Mac OS X Mountain Lion™ • Mac OS X Lion™ **Hinweis** Lokale Mac OS-Konten oder mobile Konten können die Verschlüsselung unter Mac OS X Mountain Lion oder höher einleiten. Andere Mac OS-Benutzerkontentypen sind nicht in der Lage, die Verschlüsselung einzuleiten. Informationen darüber, wie Sie ein mobiles Konto für Active Directory auf dem Mac einrichten, finden Sie unter *Mobiles Konto für Active Directory unter Mac OS erstellen auf Seite 6-22*.
Andere Software	• Mono runtime environment (MRE) 2.1 • Apple FileVault ist deaktiviert.

Systemvoraussetzungen für File Encryption

In der folgenden Tabelle werden die Systemvoraussetzungen für File Encryption beschrieben.

TABELLE 2-12. Systemvoraussetzungen für File Encryption

SPEZIFIKATION	VORAUSSETZUNGEN
Prozessor	Intel™ Core™ 2 oder kompatibler Prozessor.
RAM	• Mindestens 1GB
Festplattenspeicher	• Mindestens 30GB • 20 % freier Speicherplatz erforderlich
Netzwerkverbindung	Kommunikation mit PolicyServer für verwaltete Agents erforderlich
Betriebssystem	• Windows™ 8.1 (32 Bit/64 Bit) • Windows™ 8 (32 Bit/64 Bit) • Windows™ 7 (32 Bit/64 Bit) • Windows™ Vista mit SP1 (32 Bit/64 Bit) • Windows™ XP mit SP3 (nur 32 Bit)
Andere Software	Weitere Anforderungen für Windows 8: • Microsoft .NET Framework 3.5 aktiviert Weitere Voraussetzungen für Windows XP: • Microsoft .NET Framework 2.0 SP1 oder höher • Microsoft Windows Installer 3.1



Wichtig

Der Full Disk Encryption Agent kann nur auf einem Endpunkt mit einem einzigen physischen Laufwerk installiert werden. Entfernen Sie alle anderen Laufwerke, bevor Sie Full Disk Encryption installieren.



Kapitel 3

Übersicht über Verteilung und Upgrade

In diesem Kapitel werden die Verteilungsoptionen zusammengefasst und die technischen Voraussetzungen für die erste Verteilung der Endpoint Encryption Agents im gesamten Unternehmen, verschiedene Optionen für Skalierung und Netzwerktopologie sowie das Upgrade des gesamten Unternehmens von einer früheren Endpoint Encryption Version auf Endpoint Encryption 5.0 Patch 1 beschrieben.

Informationen zur Zusammenstellung eines Produktteams oder zu bewährten Methoden zur Kommunikation mit Endbenutzern finden Sie unter *Überlegungen zur Verteilung auf Seite B-1*.

Es werden folgende Themen behandelt:

Installation und Verteilung planen

Wenn ein Verschlüsselungsprojekt umgesetzt werden soll, ist es wichtig, die Implementierungsziele zu identifizieren. Unternehmen, die explizite Anforderungen hinsichtlich der Einhaltung gesetzlicher Bestimmungen erfüllen müssen, benötigen häufig weiter gefasste Verschlüsselungslösungen mit einem Schwerpunkt auf der Berichterstellung, während Unternehmen, die die Datensicherheit erhöhen möchten, möglicherweise gezieltere Bedürfnisse für den Schutz spezifischer Daten-Assets haben.

Ein einzelner Plan ist nicht für jedes Anwendungsszenario passend. Das Verständnis davon, was von einer Verschlüsselungslösung verlangt wird, verkürzt die Verteilungszeiten bedeutend, minimiert oder verhindert einen Leistungsabfall und stellt den Erfolg des Projekts sicher. Es ist eine sorgfältige Planung erforderlich, um die Verteilungsanforderungen und Einschränkungen für die Skalierung von Endpoint Encryptio für Endpunkte in einem großen Unternehmen zu verstehen. Die Planung ist besonders wichtig, wenn diese Änderung auf Tausenden von Endpunkten mit Auswirkungen auf alle Endbenutzer umgesetzt wird.

Checkliste vor der Verteilung

In den folgenden Tabellen werden die unterstützten Betriebssysteme und Bereitstellungsvoraussetzungen für die einzelnen Endpoint Encryption Agents aufgeführt.

TABELLE 3-1. PolicyServer 5.0 Patch 1

BETRIEBSSYSTEM	CHECKLISTE VOR DER VERTEILUNG
Windows Server 2003 (32/64-Bit-Version) Windows Server 2008/2008 R2 (64-Bit-Version)	• Installieren Sie sowohl Microsoft .NET Framework 2.0 SP2 (oder 3.5) und 4.0 • Installieren Sie mit einem Administratorkonto PolicyServer MMC • Für die Anmeldung bei PolicyServer MMC ist eine Verbindung mit der PolicyServer Datenbank erforderlich

TABELLE 3-2. Full Disk Encryption

BETRIEBSSYSTEM	CHECKLISTE VOR DER VERTEILUNG
Windows 8™ (32/64 Bit)	• Bei UEFI-kompatiblen Geräten muss die Startreihenfolge im BIOS auf **Legacy** statt **UEFI** festgelegt werden. • Vergewissern Sie sich, dass Microsoft .Net 3.5 aktiviert ist. • Führen Sie vor der Installation `sfc /scannow` und `defrag` aus. • Bestätigen Sie, dass ein normaler Master Boot Record (MBR) vorliegt. • Überprüfen Sie, ob 20 % freier Festplattenspeicher verfügbar ist. • Sichern Sie die Benutzerdaten. **Hinweis** Full Disk Encryption für Windows 8 unterstützt keine RAID-, SCSI-, eDrive- oder OPAL 2-Laufwerke.

<table>
<tr><th>Betriebssystem</th><th>Checkliste vor der Verteilung</th></tr>
<tr><td>Windows 7™ (32/64 Bit)</td><td rowspan="3">• Vergewissern Sie sich, dass Microsoft .NET 2.0 SP1 oder höher installiert ist.
• Vergewissern Sie sich, dass Windows Installer Version 3.1 installiert ist.
• Verbindung mit PolicyServer, falls verwaltet.
• Führen Sie <code>scandisk</code> und <code>defrag</code> vor der Installation aus.
• Bestätigen Sie, dass ein normaler Master Boot Record (MBR) vorliegt.
• Überprüfen Sie, ob 20 % freier Festplattenspeicher verfügbar ist.
• Sichern Sie die Benutzerdaten.

Hinweis
Full Disk Encryption unterstützt keine RAID- oder SCSI-Laufwerke.</td></tr>
<tr><td>Windows Vista™ mit SP1 (32/64 Bit)</td></tr>
<tr><td>Windows XP™ mit SP3 (32 Bit)</td></tr>
</table>

Tabelle 3-3. File Encryption

<table>
<tr><th>Betriebssystem</th><th>Checkliste vor der Verteilung</th></tr>
<tr><td>Windows 8™ (32/64 Bit)</td><td>• Bei UEFI-kompatiblen Geräten muss die Startreihenfolge im BIOS auf Legacy statt UEFI festgelegt werden.
• Vergewissern Sie sich, dass Microsoft .Net 3.5 aktiviert ist.</td></tr>
<tr><td>Windows 7™ (32/64 Bit)</td><td rowspan="3">• Vergewissern Sie sich, dass Microsoft .NET 2.0 SP1 oder höher installiert ist.</td></tr>
<tr><td>Windows Vista™ mit SP1 (32/64 Bit)</td></tr>
<tr><td>Windows XP™ mit SP3 (32 Bit)</td></tr>
</table>



Hinweis

Informationen zur Zusammenstellung eines Produktteams oder zu bewährten Methoden zur Kommunikation mit Endbenutzern finden Sie unter *Überlegungen zur Verteilung auf Seite B-1*.

Zusammenfassung der Vorgänge bei der Verteilung

Das folgende Verfahren gibt eine Übersicht über die Vorgänge, die erforderlich sind, um Endpoint Encryption 5.0 Patch 1 im gesamten Unternehmen zu verteilen.



Hinweis

Informationen zu Neuinstallationen finden Sie unter *Verteilungsoptionen auf Seite 3-12*.

Informationen zum Upgrade des Unternehmens finden Sie unter *Verteilung von Upgrades auf Seite 3-22*.

Prozedur

1. Planen Sie die Verteilung.

   Weitere Informationen finden Sie unter *Überlegungen zur Verteilung auf Seite B-1*.

2. Führen Sie ein Pilotprogramm durch.

   Weitere Informationen finden Sie unter *Pilotverteilung von Endpoint Encryption auf Seite C-1*.

3. Entscheiden Sie, wie Endpoint Encryption verwaltet werden soll.

   Weitere Informationen finden Sie unter *Verwaltungsoptionen auf Seite 3-6*.

4. Entscheiden Sie, ob eine Integration mit anderen Produkten von Trend Micro erfolgen soll.

   Weitere Informationen finden Sie unter *Integration des Control Managers auf Seite 5-1*.

Weitere Informationen finden Sie unter *Integration von OfficeScan auf Seite 7-1*.

5. Überprüfen Sie alle Systemvoraussetzungen.

   Siehe *Systemvoraussetzungen auf Seite 2-1*.

6. Installieren oder aktualisieren Sie PolicyServer.

   Weitere Informationen finden Sie unter *PolicyServer Verteilung auf Seite 4-1*.

7. Entscheiden Sie, ob die Active Directory-Authentifizierung konfiguriert werden soll.

   Weitere Informationen finden Sie unter *PolicyServer – Active Directory-Synchronisierung auf Seite 4-17*.

8. Installieren oder aktualisieren Sie Endpoint Encryption Agents.

   Weitere Informationen finden Sie unter *Verteilung von Endpoint Encryption Agents auf Seite 6-1*.

9. Verwalten Sie die Implementierung von Endpoint Encryption.

   Weitere Informationen finden Sie im *Endpoint Encryption Administratorhandbuch*.

Verwaltungsoptionen

In diesem Abschnitt wird beschrieben, wie Sie Endpoint Encryption Sicherheit nur mit der PolicyServer MMC Verwaltung verteilen oder mit Control Manager and OfficeScan integrieren, um weitere Verwaltungsoptionen zu erhalten.



Hinweis

Einführungen in die Management-Konsole finden Sie unter *Management-Konsolen auf Seite 1-15*.

Endpoint Encryption nur mit PolicyServer MMC verwalten

Das folgende Verfahren erklärt, wie Sie Endpoint Encryption konfigurieren, um nur mit PolicyServer MMC Richtlinien, Benutzer und Geräte zu verwalten, ohne die Integration in Control Manager oder OfficeScan zu nutzen.



Hinweis

Weitere Informationen finden Sie unter *PolicyServer Verteilung auf Seite 4-1*

Prozedur

1. Installieren Sie PolicyServer.

   Weitere Informationen finden Sie unter *PolicyServer installieren auf Seite 4-3*.

2. Konfigurieren Sie Gruppen.

3. Fügen Sie Benutzer jeder Gruppe hinzu.

4. Nutzen Sie Fremdprodukte, um Agents zu verteilen oder manuell auf den einzelnen Endpunkten zu installieren.

   Siehe *Verteilung von Endpoint Encryption Agents auf Seite 6-1*.

Integration von Control Manager and OfficeScan

Endpoint Encryption ermöglicht, dass Administratoren PolicyServer mit Hilfe von Trend Micro Control Manager steuern und Endpoint Encryption Agent-Richtlinien verwalten, oder mit Trend Micro OfficeScan die Endpoint Encryption AgentSoftware auf verwaltete Endpunkte verteilen.

Die Implementierung von Endpoint Encryption lässt sich in eine vorhandene Sicherheitsinfrastruktur zur Prävention von Datenverlust integrieren, die bereits von Control Manager verwaltet wird. Sie können einfach PolicyServer als verwaltetes Produkt hinzufügen, um Zugriff auf alle Aspekte der Benutzer-, Richtlinien- und Geräteverwaltung in PolicyServer MMC zu erhalten. Sie können weiterhin PolicyServer MMC für einige erweiterte Funktionen für die Unternehmensverwaltung nutzen.

In Umgebungen mit verwalteten OfficeScan Endpunkten setzen Sie das Plug-in des Endpoint Encryption Verteilungstools ein, um dezentral die Software für Endpoint Encryption Agents zu verteilen. Auch wenn traditionelle Methoden zur Verteilung der Endpoint Encryption Agent-Software weiterhin verfügbar sind (siehe *Automatisierte Verteilungen auf Seite 6-29*), ermöglicht OfficeScan die präzise Steuerung der Verteilung; Sie können den Installationsstatus der Endpoint Encryption Agents anzeigen und ohne großen Aufwand die Verteilung von einer Web-basierten Konsole aus steuern.



Hinweis

Informationen über verfügbare Management-Konsolen zur Steuerung von PolicyServer oder zur Verwaltung von Endpoint Encryption Agents finden Sie unter *Management-Konsolen auf Seite 2-6*.

Informationen zur Integration mit Control Manager finden Sie unter *Integration des Control Managers auf Seite 5-1*.

Informationen zur Integration mit OfficeScan finden Sie unter *Integration von OfficeScan auf Seite 7-1*.

Einführung in Trend Micro Control Manager

Der Trend Micro Control Manager ist eine zentrale Management-Konsole zur Verwaltung von Produkten und Services von Trend Micro auf Gateways, Mail-Servern, File-Servern und Unternehmensdesktops. Administratoren können mit den Funktionen zur Richtlinienverwaltung die Produkteinstellungen für die verwalteten Produkte und Endpunkte konfigurieren und verteilen. Die webbasierte Management-Konsole von Control Manager bietet einen zentralen Überwachungspunkt für die Verwaltung der Produkte und Dienste für Virenschutz und Content Security im gesamten Netzwerk.

Mit Control Manager kann der Systemadministrator Aktivitäten wie beispielsweise auftretende Virenausbrüche, Sicherheitsverstöße oder mögliche Viren-/Malware-Eintrittsstellen überwachen und aufzeichnen. Der Systemadministrator kann Update-Komponenten herunterladen und im Netzwerk verteilen und somit einen einheitlichen und aktuellen Schutz gewährleisten. Zu den Beispielen für Update-Komponenten zählen die Viren-Pattern-Dateien, die Scan Engine und die Anti-Spam-Regeln. Mit Control Manager sind sowohl manuelle als auch zeitgesteuerte Updates möglich. Mit Control Manager können Produkte in Gruppen oder einzeln konfiguriert und verwaltet werden.

Einführung in Trend Micro OfficeScan

OfficeScan schützt Unternehmensnetzwerke vor Malware, Netzwerkviren, webbasierten Bedrohungen, Spyware und kombinierten Bedrohungen. OfficeScan ist eine integrierte Lösung und besteht aus einem Agent am Endpunkt sowie einem Serverprogramm, das alle Agents verwaltet. Der Agent überwacht den Endpunkt und sendet dessen Sicherheitsstatus an den Server. Über die webbasierte Management-Konsole vereinfacht der Server das Festlegen koordinierter Sicherheitsrichtlinien und verteilt Updates an alle Agents.

Mit dem Plug-in für das OfficeScan Endpoint Encryption Verteilungstool können Sie die Endpoint Encryption Agents auf verwaltete OfficeScan Endpunkte verteilen. Sie können Endpunkte auf Grundlage bestimmter Kriterien auswählen und den Status der Verteilung anzeigen. Nachdem das Plug-in für das Endpoint Encryption Verteilungstool die Software für den Endpoint Encryption Agent verteilt hat, führt der Endpoint Encryption Agent eine Synchronisierung mit PolicyServer unter Verwendung der Einstellungen durch, die im Plug-in angegeben wurden. OfficeScan verwaltet keine Endpoint Encryption Richtlinien. Der OfficeScan Agent und der Endpoint Encryption Agent befinden sich unabhängig voneinander auf demselben Endpunkt.

Info über Trend Micro OfficeScan Integration

OfficeScan schützt Unternehmensnetzwerke vor Malware, Netzwerkviren, webbasierten Bedrohungen, Spyware und kombinierten Bedrohungen. OfficeScan ist eine integrierte Lösung und besteht aus einem Agent am Endpunkt sowie einem Serverprogramm, das alle Agents verwaltet. Der Agent überwacht den Endpunkt und sendet dessen Sicherheitsstatus an den Server. Über die webbasierte Management-Konsole vereinfacht der Server das Festlegen koordinierter Sicherheitsrichtlinien und verteilt Updates an alle Agents.



Hinweis

Informationen über OfficeScan finden Sie in der Begleitdokumentation unter:

http://docs.trendmicro.com/de-de/enterprise/officescan.aspx

Mit dem Plug-in für das OfficeScan Endpoint Encryption Verteilungstool können Sie die Endpoint Encryption Agents auf verwaltete OfficeScan Endpunkte verteilen. Sie

können Endpunkte auf Grundlage bestimmter Kriterien auswählen und den Status der Verteilung anzeigen. Nachdem das Plug-in für das Endpoint Encryption Verteilungstool die Software für den Endpoint Encryption Agent verteilt hat, führt der Endpoint Encryption Agent eine Synchronisierung mit PolicyServer unter Verwendung der Einstellungen durch, die im Plug-in angegeben wurden. OfficeScan verwaltet keine Endpoint Encryption Richtlinien. Der OfficeScan Agent und der Endpoint Encryption Agent befinden sich unabhängig voneinander auf demselben Endpunkt.

In der folgenden Darstellung wird illustriert, wie Sie Endpoint Encryption zum ersten Mal auf Endpunkte verteilen, die von OfficeScan verwaltet werden. In OfficeScan Installationen können Administratoren PolicyServer entweder mit Control Manager oder PolicyServer MMC verwalten.

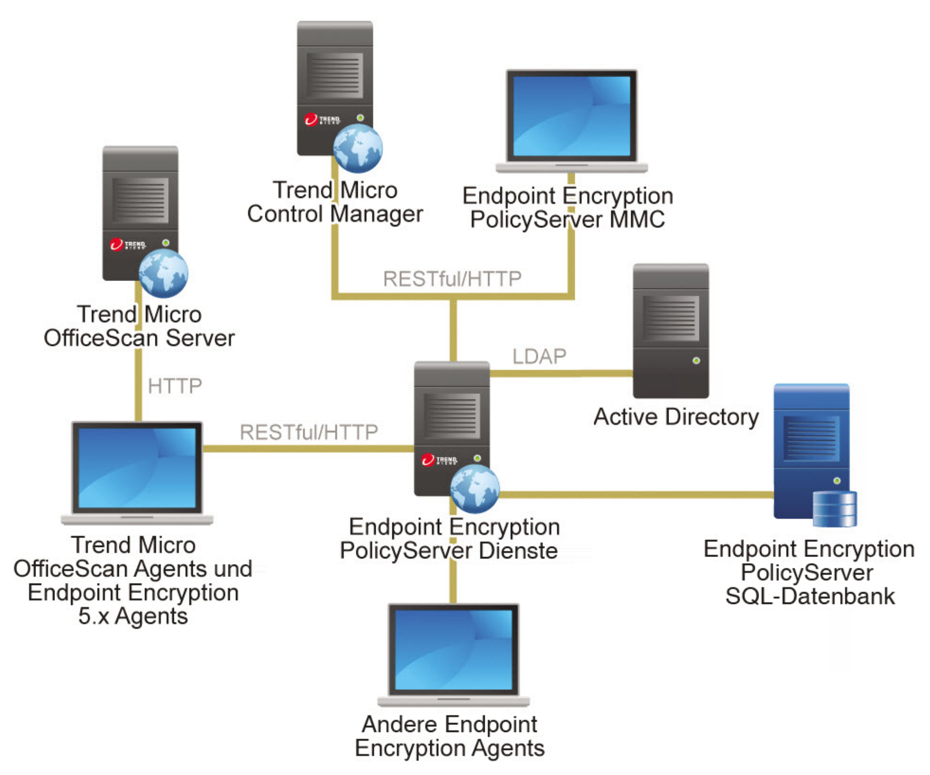


ABBILDUNG 3-1. Verteilung der OfficeScan Integration

Zusammenfassung der Vorgänge

Endpoint Encryption ermöglicht, dass Administratoren PolicyServer mit Hilfe von Trend Micro Control Manager steuern und Endpoint Encryption Agent-Richtlinien verwalten, oder mit Trend Micro OfficeScan die Endpoint Encryption AgentSoftware auf verwaltete Endpunkte verteilen. Das folgende Verfahren gibt eine Übersicht über die Vorgänge zur Installation der Management-Konsole sowie zur Verteilung der Endpoint Encryption Agent-Software und Sicherheitsrichtlinien.



Hinweis

Informationen über verfügbare Management-Konsolen zur Steuerung von PolicyServer oder zur Verwaltung von Endpoint Encryption Agents finden Sie unter *Management-Konsolen auf Seite 2-6*.

Informationen zur Integration mit Control Manager finden Sie unter *Integration des Control Managers auf Seite 5-1*.

Informationen zur Integration mit OfficeScan finden Sie unter *Integration von OfficeScan auf Seite 7-1*.

Prozedur

1. Überprüfen Sie alle Systemvoraussetzungen für kompatible Produktversionen.

   Weitere Informationen finden Sie unter *Systemvoraussetzungen auf Seite 2-1*.

2. Installieren Sie PolicyServer.

   Weitere Informationen finden Sie unter *PolicyServer installieren auf Seite 4-3*.

3. Installieren und konfigurieren Sie OfficeScan.

   Die begleitende Dokumentation finden Sie unter:

   http://docs.trendmicro.com/de-de/enterprise/officescan.aspx

4. Fügen Sie PolicyServer zu OfficeScan hinzu.

   Weitere Informationen finden Sie unter *Servereinstellungen verteilen auf Seite 7-11*.

5. Bereiten Sie die Endpunkte für die Verteilung vor.

Weitere Informationen finden Sie unter *Vor der Installation von Endpoint Encryption Agents auf Seite 6-5*.

6. Verteilen Sie die Endpoint Encryption Agents mit OfficeScan.

   Siehe *Integration von OfficeScan auf Seite 7-1*.

7. Installieren und Konfigurieren von Control Manager.

   Die begleitende Dokumentation finden Sie unter:

   http://docs.trendmicro.com/en-us/enterprise/control-manager.aspx

8. Fügen Sie PolicyServer zu Control Manager hinzu.

   Siehe *PolicyServer als verwaltetes Produkt zu Control Manager hinzufügen auf Seite 5-4*.

9. Verteilen Sie die Richtlinien mit Control Manager.

   Weitere Informationen finden Sie unter *Eine Richtlinie erstellen auf Seite 5-8*.

Verteilungsoptionen

Wenn Sie Endpoint Encryption im gesamten Unternehmen verteilen möchten, sind abhängig von der vorhandenen Infrastruktur und den Sicherheitsanforderungen mehrere Netzwerkoptionen verfügbar. In diesem Abschnitt werden die verfügbaren Verteilungsoptionen für die Endpoint Encryption Verteilung beschrieben.

Einfache Verteilung

Die folgende Darstellung illustriert, wie Sie Endpoint Encryption zum ersten Mal verteilen und nur PolicyServer MMC zur Verwaltung von PolicyServer verwenden.

Weitere Informationen finden Sie unter *Installation und Konfiguration von PolicyServer auf Seite 4-3*.

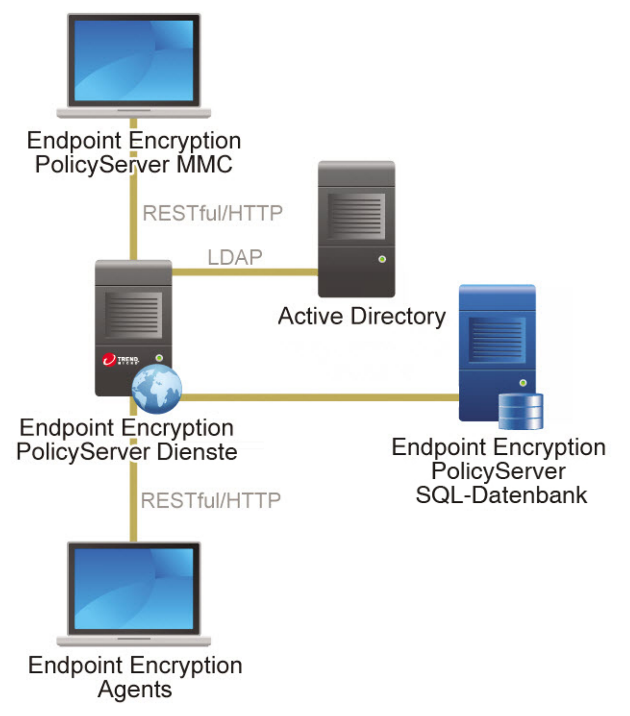


ABBILDUNG 3-2. Einfache Verteilung von Endpoint Encryption



Hinweis

Informationen über eine Upgrade-Verteilung, bei der möglicherweise Endpoint Encryption 3.1.3 (oder ältere) Agents beteiligt sind, finden Sie unter *Verteilung von Upgrades auf Seite 3-22*.

Control Manager Verteilung

Die folgende Darstellung illustriert, wie Sie Endpoint Encryption zum ersten Mal verteilen und Control Manager zur Verwaltung von PolicyServer verwenden. In einer

Control Manager Installation setzen Administratoren Control Manager für alle Endpoint Encryption Richtlinien, Benutzer und Gerätefunktionen ein und verwenden PolicyServer MMC nur für die erweiterte Unternehmenswartung.

Weitere Informationen finden Sie unter *Integration des Control Managers auf Seite 5-1*.

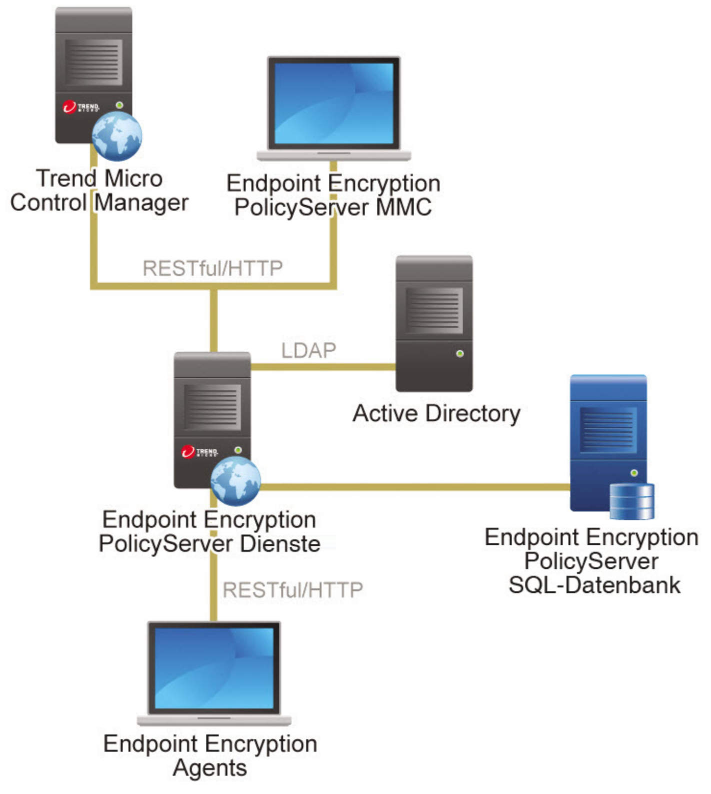


ABBILDUNG 3-3. Verteilung der Control Manager Integration



Hinweis

In Umgebungen, in denen Control Manager eingesetzt wird, werden Änderungen an PolicyServer Richtlinien immer von Control Manager gesteuert. Alle mit PolicyServer MMC durchgeführten Änderungen werden beim nächsten Mal überschrieben, wenn Control Manager die Richtlinien mit der PolicyServer Datenbank synchronisiert.

OfficeScan Verteilung

In der folgenden Darstellung wird illustriert, wie Sie Endpoint Encryption zum ersten Mal auf Endpunkte verteilen, die von OfficeScan verwaltet werden. In OfficeScan Installationen können Administratoren PolicyServer entweder mit Control Manager oder PolicyServer MMC verwalten.

Weitere Informationen finden Sie unter *Integration von OfficeScan auf Seite 7-1*

ABBILDUNG 3-4. Verteilung der OfficeScan Integration

Komplexe verteilte Verteilung

Im folgenden Diagramm wird die Netzwerkumgebung für eine komplexe Verteilung sowohl mit Endpoint Encryption 5.0 Patch 1 als auch älteren Endpoint Encryption Agents beschrieben. Sie können Traffic Forwarding Service und Client-Web-Service auf

demselben Endpunkt gesondert von PolicyServer konfigurieren. Weitere Informationen finden Sie unter *Services auf mehreren Endpunkten konfigurieren auf Seite 4-25*.

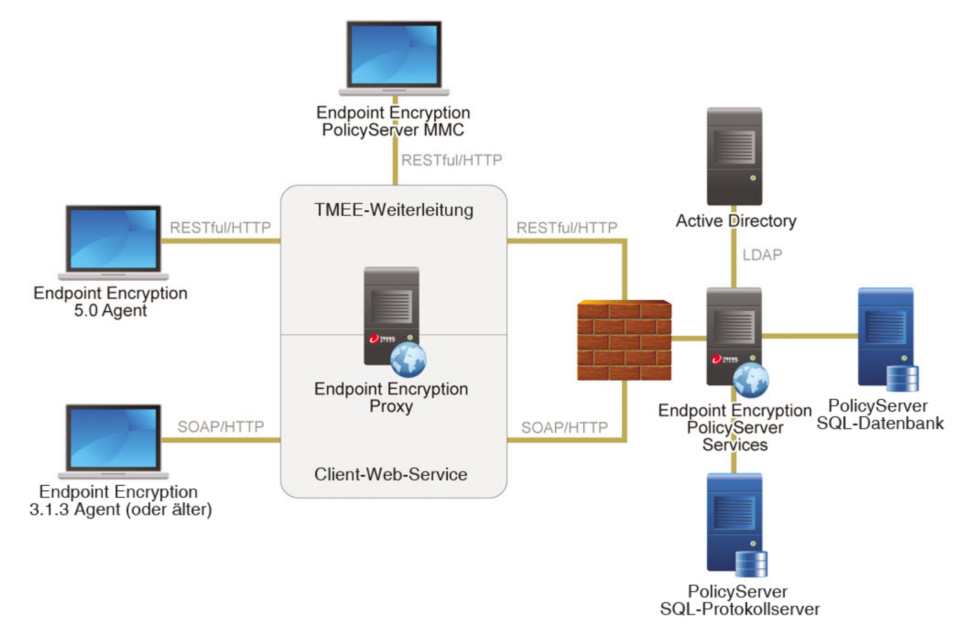


ABBILDUNG 3-5. Komplexe verteilte Verteilung

Empfehlungen zur Skalierung

Nachfolgend finden Sie Empfehlungen für die Skalierung an einem einzelnen Standort, die verschiedene Hardware-Optionen für die Systemredundanz und keinen "Single Point of Failure" bietet.

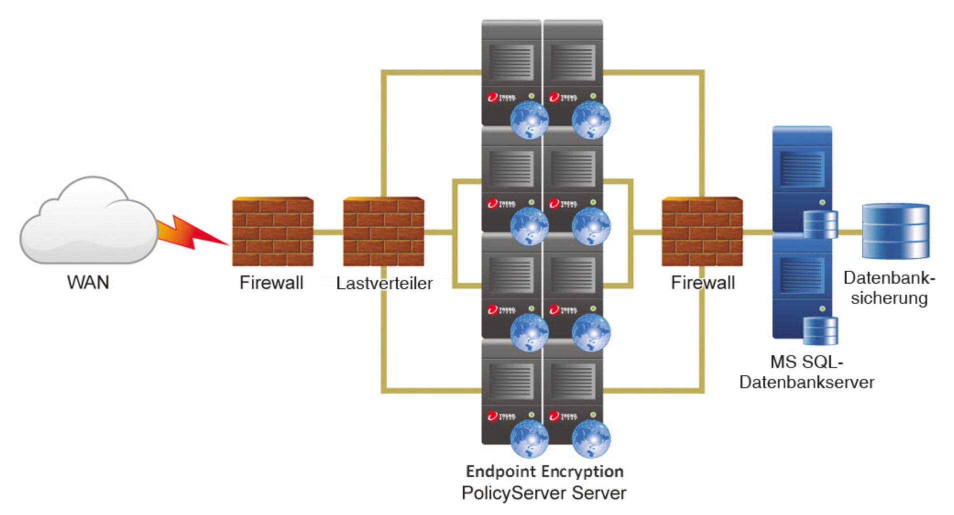


Abbildung 3-6. PolicyServer für die Unterstützung von 40.000 Benutzern skaliert

Tabelle 3-4. Skalierung ohne Redundanz

Geräte	Mindestsystemvoraussetzungen	
	PolicyServer Frontend	PolicyServer SQL Datenbank
1,500	• PolicyServer und Datenbank-Mehrzweck-Server • 2 GHz Quad Core Core2 Intel™ Xeon™ Prozessoren • 8GB Arbeitsspeicher • 120GB RAID 5 Festplattenspeicher	• Installiert auf PolicyServer Frontend-Host

Geräte	Mindestsystemvoraussetzungen	
	PolicyServer Frontend	PolicyServer SQL Datenbank
3,000	• 1 PolicyServer Frontend-Host • 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Prozessoren • 4GB Arbeitsspeicher • 40GB RAID 1 Festplattenspeicher	• 1 PolicyServer SQL Datenbank-Host • 2 GHz Quad Core Core2 Intel™ Xeon™ Prozessoren • 8GB Arbeitsspeicher • 100GB RAID 5 Festplattenspeicher

Tabelle 3-5. Skalierung mit Redundanz und hoher Verfügbarkeit

Geräte	Mindestsystemvoraussetzungen	
	PolicyServer Frontend	PolicyServer SQL Datenbank
10,000	• 2 PolicyServer Frontend-Hosts • 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Prozessoren • 4GB Arbeitsspeicher • 40GB RAID 1 Festplattenspeicher	• 1 PolicyServer SQL Datenbank-Hosts • 2 GHz Quad Core Core2 Intel™ Xeon™ Prozessoren • 8GB Arbeitsspeicher • 120GB RAID 5 Festplattenspeicher
20,000	• 4 PolicyServer Frontend-Hosts • 2 GHz Dual Quad Core2 Intel™ Xeon™ Prozessoren • 4GB Arbeitsspeicher • 40GB RAID 1 Festplattenspeicher	• 1 PolicyServer SQL Datenbank-Hosts • 2 GHz Quad Core2 Intel™ Xeon™ Prozessoren • 16GB Arbeitsspeicher • 160GB RAID 5 Festplattenspeicher

Geräte	Mindestsystemvoraussetzungen	
	PolicyServer Frontend	PolicyServer SQL Datenbank
40,000	• 8 PolicyServer Frontend-Hosts • 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Prozessoren • 4GB Arbeitsspeicher • 40GB RAID 1 Festplattenspeicher	• 2 PolicyServer SQL Datenbank-Cluster-Hosts • 2 GHz Quad Core Core2 Intel™ Xeon™ Prozessoren • 16GB Arbeitsspeicher • 320GB RAID 5 Festplattenspeicher

Tabelle 3-6. Skalierung ohne "Single Point of Failure"

Geräte	Mindestsystemvoraussetzungen	
	PolicyServer Frontend	PolicyServer SQL Datenbank
10,000	• 2 PolicyServer Frontend-Hosts • 2 GHz Quad Core Core2 Intel™ Xeon™ Prozessoren • 4GB Arbeitsspeicher • 40GB RAID 1 Festplattenspeicher **Hinweis** Virtualisierte Hardware wird unter VMware Virtual Infrastructure unterstützt.	• 2 PolicyServer SQL Datenbank-Hosts • 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Prozessoren • 8GB Arbeitsspeicher • 60GB RAID 5 Festplattenspeicher • 130GB Festplattenspeicher auf gemeinsam genutzten RAID 5 SAN **Hinweis** Microsoft oder VMware auf virtualisierter Hardware bietet keine Unterstützung für den Microsoft Cluster Service.

<table>
<tr><th rowspan="2">GERÄTE</th><th colspan="2">MINDESTSYSTEMVORAUSSETZUNGEN</th></tr>
<tr><th>POLICYSERVER FRONTEND</th><th>POLICYSERVER SQL DATENBANK</th></tr>
<tr><td>20,000</td><td>• 4 PolicyServer Frontend-Hosts
• 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Prozessoren
• 4GB Arbeitsspeicher
• 40GB RAID 1 Festplattenspeicher

Hinweis
Virtualisierte Hardware wird unter VMware Virtual Infrastructure unterstützt.</td><td>• 2 PolicyServer SQL Datenbank-Hosts
• 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Prozessoren
• 8GB Arbeitsspeicher
• 60GB RAID 5 Festplattenspeicher
• 180GB Festplattenspeicher auf gemeinsam genutzten RAID 5 SAN

Hinweis
Microsoft oder VMware auf virtualisierter Hardware bietet keine Unterstützung für den Microsoft Cluster Service.</td></tr>
</table>

<table>
<tr><th rowspan="2">Geräte</th><th colspan="2">Mindestsystemvoraussetzungen</th></tr>
<tr><th>PolicyServer Frontend</th><th>PolicyServer SQL Datenbank</th></tr>
<tr><td>40,000</td><td>• 8 PolicyServer Frontend-Hosts
• 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Prozessoren
• 4GB Arbeitsspeicher
• 40GB RAID 1 Festplattenspeicher

Hinweis
Virtualisierte Hardware wird unter VMware Virtual Infrastructure unterstützt.</td><td>• 4 PolicyServer SQL Datenbank-Hosts
• 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Prozessoren
• 16GB Arbeitsspeicher
• 60GB RAID 5 Festplattenspeicher
• 350GB Festplattenspeicher auf gemeinsam genutzten RAID 5 SAN

Hinweis
Microsoft oder VMware auf virtualisierter Hardware bietet keine Unterstützung für den Microsoft Cluster Service.</td></tr>
</table>

Verteilung von Upgrades

Um Zugriff auf neue Produktfunktionen zu erhalten oder eine ältere Agent-Software zu aktualisieren, um die Endpunktsicherheit zu verbessern, müssen Administratoren möglicherweise den Endpoint Encryption PolicyServer und alle verwalteten Endpunkte aktualisieren, auf denen ein Endpoint Encryption Agent ausgeführt wird. Um die Synchronisierung der Richtlinien und die Sicherheit der Informationen zu gewährleisten, müssen Sie PolicyServer immer vor den Endpoint Encryption Agents aktualisieren.

In diesem Abschnitt wird beschrieben, wie auf sichere Weise ein Upgrade von Endpoint Encryption, einschließlich PolicyServer, PolicyServer MMC und der Software für den Endpoint Encryption Agent, auf die neuesten Versionen durchgeführt werden kann. Weitere Informationen finden Sie unter *Zusammenfassung der Vorgänge zu Upgrades auf Seite 3-26*

Überlegungen zum Upgrade

Die folgende Darstellung zeigt das Erscheinungsbild des ursprünglichen Upgrades, bevor alle Endpoint Encryption Agents auf den Endpoint Encryption 5.0 Patch 1 Agent aktualisiert wurden.

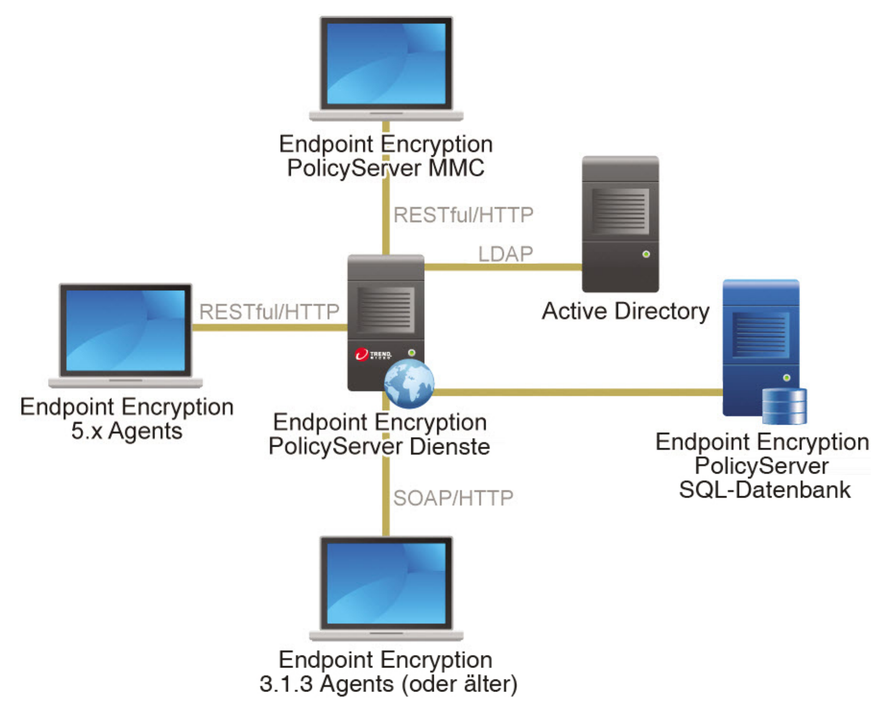


ABBILDUNG 3-7. Upgrade-Verteilung von Endpoint Encryption



Hinweis

Informationen zur Kommunikation von Endpoint Encryption Agents finden Sie unter *Info über PolicyServer auf Seite 1-13*.

Bevor Sie PolicyServer upgraden, beachten Sie Folgendes:

- Vergewissern Sie sich, dass PolicyServer vor der Aktualisierung der Endpoint Encryption Agents aktualisiert wird. Informationen zur korrekten Upgrade-Reihenfolge finden Sie unter *Zusammenfassung der Vorgänge zu Upgrades auf Seite 3-26*.
- Das Upgrade von Umgebungen mit mehreren PolicyServer Instanzen stellt andere Anforderungen als eine Umgebung mit nur einem PolicyServer. Weitere Informationen finden Sie unter *Upgrades für mehrere PolicyServer Dienste installieren, die mit derselben Datenbank verbunden sind auf Seite 4-35*.
- Wenn ein LDAP-Proxy verwendet wird, führen Sie erst das Upgrade des LDAP-Proxy durch, bevor Sie das Upgrade auf PolicyServer 5.0 Patch 1 aufspielen.



Hinweis

Trend Micro unterstützt gehostete PolicyServer Umgebungen zurzeit nicht.

Upgrade-Pfade

In der folgenden Tabelle werden die Upgrade-Pfade von jeder früheren Produktversion bis Version 5.0 Patch 1 beschrieben. Einige ältere Versionen können nicht direkt auf 5.0 Patch 1 aktualisiert, sondern müssen zunächst auf eine neuere Version des Produkts aktualisiert werden. Informationen zur Installation von älteren Versionen von Endpoint Encryption finden Sie in der Dokumentation, die Sie unter folgender Adresse herunterladen können:

http://docs.trendmicro.com/de-de/enterprise/endpoint-encryption.aspx.

TABELLE 3-7. Upgrade-Pfade

PRODUKT/AGENT	VERSION	UPGRADE-PFAD
PolicyServer	3.1.3 SP1	3.1.3 SP1 → 5.0
	3.1.3	3.1.3 → 5.0
	3.1.2	3.1.2 → 5.0
Full Disk Encryption	3.1.3 SP1	3.1.3 SP1 → 5.0
	3.1.3	3.1.3 → 5.0

Produkt/Agent	Version	Upgrade-Pfad
MobileArmor Full Disk Encryption	3.1.2	3.1.2 → Full Disk Encryption 5.0
	SP7g	SP7g → 3.1.3 → Full Disk Encryption 5.0
	SP7-SP7f	SP7-SP7f → SP7g → 3.1.3 → Full Disk Encryption 5.0
DriveArmor	3.0	Nicht unterstützt
FileArmor	3.1.3 SP1	FileArmor 3.1.3 SP1 → File Encryption 5.0
	3.1.3	FileArmor 3.1.3 → File Encryption 5.0
	3.0.14	FileArmor 3.0.14 → FileArmor 3.1.3 → File Encryption 5.0
	3.0.13	FileArmor 3.0.13 → FileArmor 3.1.3 → File Encryption 5.0
KeyArmor	3.0.2	Es gibt keine KeyArmor 5.0 Version.
	3.0.1	

Unterstützte Agent-Versionen

Obwohl PolicyServer die Richtlinienverwaltung für alle Agents unterstützt, können sich ältere Agents nicht als neues Gerät bei PolicyServer 5.0 Patch 1 oder Control Manager registrieren. In der folgenden Tabelle wird erklärt, welche ältere Versionen als neues Gerät hinzugefügt werden können. Trend Micro empfiehlt die Verwendung der neuesten Versionen für alle Agents.

TABELLE 3-8. Unterstützte ältere Agents für neue Geräte

AGENT	VERSION	KANN ALS NEUES GERÄT REGISTRIERT WERDEN	UNTERSTÜTZE RICHTLINIEN
Full Disk Encryption	5.0	●	●
	3.1.3 SP1	●	●
	3.1.3	●	●
MobileArmor Full Disk Encryption	3.1.2		●
	SP7g		●
DriveArmor	3.0		●*
File Encryption	5.0 Patch 1	●	●
FileArmor	3.1.3	●	●
	3.0.14		●
	3.0.13		●
KeyArmor	Alle		●*



Hinweis

*Wird nur auf PolicyServer Upgrades von Endpoint Encryption 3.1.2 oder 3.1.3 unterstützt.

Zusammenfassung der Vorgänge zu Upgrades

Um das Risiko zu vermindern, dass Endpunkte die Verbindung mit PolicyServer verlieren, aktualisieren Sie die Umgebung in der folgenden Reihenfolge. Wenn der Agent nach dem Upgrade keine Verbindung zu PolicyServer aufbauen kann, führen Sie auf dem Endpunkt das Installationsprogramm für das Upgrade manuell aus.

Prozedur

1. Überprüfen Sie die neuen Systemvoraussetzungen.

   Weitere Informationen finden Sie unter *Systemvoraussetzungen auf Seite 2-1*.

2. Sehen Sie den Upgrade-Pfad für den momentan installierten PolicyServer und die Endpoint Encryption Agents durch.

3. Vergewissern Sie sich, dass das Upgrade von Endpoint Encryption 5.0 Patch 1 unterstützt wird.

   Weitere Informationen finden Sie unter *Unterstützte Agent-Versionen auf Seite 3-25*.

4. Aktualisieren Sie PolicyServer.

   Weitere Informationen finden Sie unter *Überlegungen zum Upgrade auf Seite 3-23*.

   Weitere Informationen finden Sie unter *Upgrade von PolicyServer auf Seite 4-31*.

5. Installieren und konfigurieren Sie optional Control Manager.

   Weitere Informationen finden Sie unter *Integration von OfficeScan auf Seite 7-1*.

6. Installieren und konfigurieren Sie optional OfficeScan.

   Weitere Informationen finden Sie unter *Integration des Control Managers auf Seite 5-1*.

7. Aktualisieren Sie die Endpoint Encryption Agents.

   Weitere Informationen finden Sie unter *Upgrade auf Seite 6-38*.



Kapitel 4

PolicyServer Verteilung

Dieses Kapitel gibt einen Überblick über die Installation von PolicyServer sowie über die Dateien und Konten, die hierfür benötigt werden.



Hinweis

Informationen zu den Systemvoraussetzungen finden Sie unter *Voraussetzungen für PolicyServer auf Seite 2-2*.

Es werden folgende Themen behandelt:

Info über PolicyServer

Trend Micro PolicyServer verwaltet Verschlüsselungsschlüssel und synchronisiert Richtlinien mit allen Endpunkten im Unternehmen. PolicyServer setzt ferner die sichere Authentifizierung durch und umfasst Echtzeit-Audits und Tools zur Berichterstellung, um die Einhaltung von gesetzlichen Bestimmungen sicherzustellen. Sie können PolicyServer with PolicyServer MMC oder mit Trend Micro Control Manager flexibel verwalten. Andere Funktionen zur Datenverwaltung umfassen benutzerseitige Selbsthilfe-Optionen und Geräteaktionen, um ein verlorenes oder gestohlenes Gerät von einem entfernten Standort aus zurückzusetzen oder „auszulöschen".

In der folgenden Tabelle werden die Komponenten von PolicyServer beschrieben, die Sie abhängig von den Anforderungen in der Umgebung auf einem oder mehreren Servern verteilen können.

TABELLE 4-1. Komponenten von PolicyServer

KOMPONENTE	BESCHREIBUNG
Unternehmen	"Endpoint Encryption - Unternehmen" ist der eindeutige Bezeichner für das Unternehmen in der PolicyServer Datenbank, der bei der Installation von PolicyServer konfiguriert wurde. In einer PolicyServer Datenbank darf es nur eine Unternehmenskonfiguration geben.
Datenbank	In der Microsoft SQL-Datenbank von PolicyServer werden alle Benutzer, Geräte und Protokolldaten sicher gespeichert. Die Datenbank ist entweder auf einem dedizierten Server konfiguriert oder wird einem vorhandenen SQL-Cluster hinzugefügt. Die Protokoll- und anderen Datenbanken können sich an unterschiedlichen Speicherorten befinden.
PolicyServer Windows-Dienst	Der PolicyServer Windows-Dienst verwaltet alle Kommunikationstransaktionen zwischen Host-Betriebssystem, Endpoint Encryption Dienst, Legacy Web-Service, Client Web Proxy und SQL-Datenbanken.

Komponente	Beschreibung
Endpoint Encryption Dienst	Alle Endpoint Encryption 5.0 Patch 1 Agents nutzen den Endpoint Encryption Dienst zur Kommunikation mit PolicyServer. Der Endpoint Encryption Dienst verwendet eine Representational State Transfer Web-API (RESTful) mit einem AES-GCM-Verschlüsselungsalgorithmus. Nachdem sich ein Benutzer authentifiziert hat, generiert PolicyServer ein Token im Zusammenhang mit der spezifischen Richtlinienkonfiguration. Bis zur Authentifizierung durch den Endpoint Encryption Benutzer sperrt der Dienst alle Richtlinientransaktionen. Um eine dreistufige Netzwerktopographie zu erstellen, kann der Dienst auch gesondert auf einen Endpunkt verteilt werden, der sich in der Netzwerk-DMZ befindet. Dadurch kann sich PolicyServer sicher hinter der Firewall befinden.
Legacy Web-Service	Alle Agents von Endpoint Encryption 3.1.3 und niedriger verwenden das Simple Object Access Protocol (SOAP), um mit PolicyServer zu kommunizieren. In bestimmten Situationen erlaubt SOAP möglicherweise unsichere Richtlinientransaktionen ohne Benutzerauthentifizierung. Legacy Web Service filtert SOAP-Aufrufe, indem eine Authentifizierung erforderlich gemacht wird und die Befehle begrenzt werden, die SOAP akzeptiert. Um eine dreistufige Netzwerktopographie zu erstellen, kann der Dienst auch gesondert auf einen Endpunkt verteilt werden, der sich in der Netzwerk-DMZ befindet. Dadurch kann sich PolicyServer sicher hinter der Firewall befinden.

Installation und Konfiguration von PolicyServer

In diesem Abschnitt wird beschrieben, wie Sie PolicyServer zum ersten Mal installieren und konfigurieren, Active Directory einrichten und den LDAP-Proxy konfigurieren.

PolicyServer installieren

Der Installationsprozess von PolicyServer beinhaltet die Ausführung des Installationsprogramms auf dem Server-Endpunkt, um Folgendes zu konfigurieren:

- Endpoint Encryption Produktlizenz
- Name des Unternehmens und Administrator-Anmeldung
- Endpoint Encryption Dienste
- PolicyServer Datenbank
- PolicyServer MMC (optional)



Hinweis

Informationen zur Architektur finden Sie unter *Komponenten von Endpoint Encryption auf Seite 1-10*. PolicyServer MMC kann optional gleichzeitig installiert werden.



Warnung!

Aus Sicherheitsgründen können ältere Endpoint Encryption Agents nicht direkt mit einer PolicyServer Instanz kommunizieren, die sich in einem anderen Netzwerk befindet. Informationen zur Konfiguration eines Web-Proxys finden Sie unter *Services auf mehreren Endpunkten konfigurieren auf Seite 4-25*.

Prozedur

1. Vergewissern Sie sich, dass alle Systemvoraussetzungen erfüllt werden.

   Weitere Informationen finden Sie unter *Voraussetzungen für PolicyServer auf Seite 2-2*.

2. Führen Sie `PolicyServerInstaller.exe` aus.

   Das PolicyServer Installationsprogramm wird geöffnet.

3. Klicken Sie im Fenster **PolicyServer Dienste** rechts auf **Installieren**.

4. Lesen Sie im Fenster **Rechtliche Hinweise zum Produkt** die Lizenzvereinbarung, und akzeptieren Sie die Bedingungen, indem Sie auf **Zustimmen** klicken.

5. Führen Sie im Fenster **Produktaktivierung** Folgendes durch:

   - Klicken Sie auf **Online registrieren**, um die Lizenz zu registrieren.

- Wählen Sie **Lizenz für eine Vollversion verwenden**, um den Aktivierungscode einzugeben und die volle Funktionalität freizuschalten.
- Wählen Sie **Testlizenz verwenden**, um die verwaltete Endpoint Encryption Konfiguration 30 Tage lang auszuprobieren.



Hinweis

Während des Testzeitraums funktioniert PolicyServer mit allen Funktionen für die Agent-Verwaltung, einer unbegrenzten Zahl von Geräten und bis zu 100 Benutzern. Weitere Informationen über Registrierungsschlüssel und Aktivierungscode erhalten Sie bei Ihrem Trend Micro Vertriebspartner, an den Sie sich nach 30 Tagen wenden sollten. Weitere Informationen zur Umwandlung der Testlizenz in eine Lizenz für eine Vollversion finden Sie unter *Neue Produktlizenz aktivieren auf Seite 8-3*.

6. Geben Sie im Fenster **Unternehmensnamen und Administrator-Anmeldung erstellen** die folgenden Anmeldedaten ein, die zur Verwaltung von PolicyServer über PolicyServer MMC oder Control Manager verwendet werden.

Option	Bezeichnung
Der Name des Unternehmens	Der Name der Datenbankinstanz.
Administrator	Der Benutzername für das neue Unternehmensadministratorkonto.
Kennwort	Das Kennwort für das neue Unternehmensadministratorkonto.
Kennwort bestätigen	Bestätigen Sie das Kennwort für das neue Unternehmensadministratorkonto.

7. Klicken Sie auf **Fortfahren**.
8. Klicken Sie im Fenster **Anmeldung beim Windows-Dienst** auf **Fortfahren**. Die Standardeinstellungen eignen sich für die meisten Umgebungen.
9. Führen Sie Folgendes im Fenster **Datenbankadministrator-Anmeldung** durch:
   - Wählen Sie **Microsoft SQL Express**, um eine neue Datenbankinstanz zu erstellen.



Hinweis

Microsoft SQL Express ist nur in Umgebungen verfügbar, in denen SQL Server nicht konfiguriert ist.

- Wählen Sie **SQL Server**, um eine Microsoft SQL Server-Instanz anzugeben, und legen Sie anschließend die folgenden Parameter fest:
  - **SQL Server**: Der Host-Name und die IP-Adresse von SQL Server.

    Hinweis

    Bei Umgebungen mit mehreren SQL Server-Instanzen fügen Sie die SQL-Instanz ans Ende des PolicyServer Hostnamens oder die verwendete IP-Adresse an. Verwenden Sie zur Angabe einer Instanz die folgende Syntax:

    ```
    <Host-Name_oder_IP-Adresse>\<Datenbankinstanz>
    ```

  - **Benutzername:** Der Benutzername mit der Rolle **sysadmin** für die angegebene SQL Server-Instanz.
  - **Kennwort**: Das Kennwort für das Konto **sysadmin**.
- Wählen Sie **Verwenden Sie einen anderen Protokolldatenbank-Server**, um eine andere SQL Server-Instanz für Protokolldaten auszuwählen.

10. Klicken Sie auf **Fortfahren**.

Das Installationsprogramm überprüft die Datenbankverbindung.

11. Geben Sie im Fenster **Datenbankanmeldung** ein neues Datenbankkonto für den PolicyServer Windows-Dienst an, das für alle Datenbanktransaktionen verwendet werden soll.



Hinweis

Geben Sie nicht das **sysadmin**-Konto an.

12. Geben Sie im Fenster **Endpoint Encryption Dienst** die folgenden Parameter ein:

Option	Bezeichnung
Portnummer	Geben Sie die Portnummer an, die PolicyServer MMC, Control Manager und Endpoint Encryption 5.0 Patch 1 Agents zur Kommunikation mit PolicyServer verwenden (Standard: 8080). **Hinweis** In Umgebungen mit älteren Agents empfiehlt Trend Micro die Verwendung von Port 8080 für den Admin-Web-Dienst und Port 80 für den Client-Web-Service. Die Portnummer muss eine positive Ganzzahl zwischen 1 und 65535 sein.
Automatisch ein neues selbstsigniertes Zertifikat generieren	Wählen Sie diese Option, wenn kein Zertifikat verfügbar ist. Das Installationsprogramm generiert ein Zertifikat für die Kommunikation.
Ein vorhandenes Zertifikat angeben	Wählen Sie diese Option, um ein bestimmtes Zertifikat zu verwenden. Es gibt keine Einschränkungen oder Voraussetzungen für die Angabe eines vorhandenen Zertifikats, außer dass das Zertifikat korrekt formatiert ist.



Hinweis

Der Endpoint Encryption Dienst verwendet eine Web-API (RESTful) zur Authentifizierung von Agents, die eine Verbindung mit PolicyServer erstellen.

13. Klicken Sie auf **Fortfahren**.

14. Wählen Sie im Fenster **Legacy-Agent-Service** den Speicherort, den die älteren Endpoint Encryption Agents (Version 3.1.3 und niedriger) zur Kommunikation mit PolicyServer nutzen, und klicken Sie anschließend auf **Fortfahren**.

15. Um PolicyServer MMC sofort zu installieren, klicken Sie auf **Ja**. Wenn Sie PolicyServer MMC zu einem späteren Zeitpunkt oder auf einem separaten Endpunkt installieren möchten, lesen Sie *PolicyServer MMC installieren auf Seite 4-9*.

    Der Installationsvorgang wird gestartet.

16. Wenn Sie dazu aufgefordert werden, klicken Sie auf **OK**.

17. Klicken Sie auf **Beendet**.

18. Klicken Sie auf **Beenden**, um das PolicyServer Installationsprogramm zu schließen.

19. Starten Sie den Server neu.

20. Fügen Sie die anfänglichen Endpoint Encryption Benutzer und Gruppen hinzu.

    Weitere Informationen finden Sie unter *PolicyServer konfigurieren auf Seite 4-8*.

PolicyServer konfigurieren

Das folgende Verfahren beschreibt, wie Sie das PolicyServer Unternehmen mit PolicyServer MMC konfigurieren. Während der Installation von PolicyServer wurden das Unternehmen und die Anmeldedaten des Unternehmensadministrators konfiguriert.



Hinweis

Informationen über die in Endpoint Encryption verfügbaren Management-Konsolen finden Sie unter *Management-Konsolen auf Seite 1-15*.

Prozedur

1. Falls noch nicht während der Installieren von PolicyServer geschehen, installieren Sie PolicyServer MMC.

   Weitere Informationen finden Sie unter *PolicyServer MMC installieren auf Seite 4-9*.

2. Melden Sie sich bei PolicyServer MMC an.

   Weitere Informationen finden Sie unter *PolicyServer MMC installieren auf Seite 4-9*.

3. Fügen Sie die erste Top-Gruppe hinzu.

   Weitere Informationen finden Sie unter *Top-Gruppe hinzufügen auf Seite 4-12*.

4. Fügen Sie Endpoint Encryption Benutzer hinzu.

   Weitere Informationen finden Sie unter *Neuen Benutzer zu einer Gruppe hinzufügen auf Seite 4-14*.

5. Erlauben Sie bestimmten Endpoint Encryption Benutzern, neue Endpoint Encryption Geräte der Gruppe hinzufügen zu dürfen.

   Weitere Informationen finden Sie unter *Einem Benutzer das Installieren in eine Gruppe erlauben auf Seite 4-17*.

PolicyServer MMC installieren

PolicyServer MMC kann optional während der Installation von PolicyServer installiert werden. In Umgebungen, in denen PolicyServer MMC und PolicyServer nicht gemeinsam eingesetzt werden, führen Sie das folgende Verfahren durch, um PolicyServer MMC zu installieren.



Hinweis

Aufgrund der verbesserten Sicherheit ist es nicht möglich, PolicyServer 5.0 Patch 1 mit älteren Versionen von PolicyServer MMC zu verwalten.

Prozedur

1. Starten Sie `PolicyServerMMCSnapinSetup.msi`.

   Die Installation beginnt.

2. Klicken Sie auf **Weiter**, um den Setup-Assistenten zu starten.

3. Lesen Sie die Lizenzvereinbarung, und akzeptieren Sie die Bedingungen, indem Sie **Ich stimme zu** auswählen. Klicken Sie anschließend auf **Weiter**.

4. Wählen Sie den Installationsordner aus oder verwenden Sie den vorgegebenen Speicherort, und klicken Sie auf **Weiter**.

5. Klicken Sie auf **Weiter**, um die Installation zu bestätigen.

   Beachten Sie im Anschluss an die Installation Folgendes:

   - Auf dem Desktop wird die Verknüpfung "PolicyServer MMC" angezeigt.

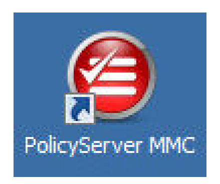


ABBILDUNG 4-1. Verknüpfung für PolicyServer MMC

- Abhängig vom Prozessor sind die Programmdateien unter `C:\Program Files\Trend Micro\PolicyServer MMC\` oder `C:\Program Files (x86)\Trend Micro\PolicyServer MMC\` installiert.

6. Klicken Sie zum Abschluss auf **Schließen**.

7. Klicken Sie auf **Ja**, um den Server neu zu starten.

8. Melden Sie sich wieder beim Server an, und öffnen Sie PolicyServer MMC, in dem Sie auf die Desktop-Verknüpfung doppelklicken.

9. Nach dem Öffnen von PolicyServer MMC authentifizieren Sie sich mit dem Unternehmensadministratorkonto, das bei der Installation der PolicyServer Datenbanken und Dienste erstellt wurde. Der 30-Tage-Testzeitraum ermöglicht unbegrenzte Geräte und bis zu 100 Benutzer.

Eine Liste der empfohlenen Aufgaben nach der Installation, z. B. Geräte und Benutzer erstellen sowie Richtlinien festlegen, finden Sie im *Endpoint Encryption Administratorhandbuch*.



Tipp

Trend Micro empfiehlt, zur Sicherheit ein zweites Unternehmensadministratorkonto zu erstellen und das Standardkennwort zu ändern.

Bei PolicyServer MMC anmelden

Sie können den Namen des Unternehmens und das Unternehmensadministratorkonto während der Installation von PolicyServer konfigurieren. Informationen über die kostenlose Testlizenz für 30 Tage finden Sie unter *Testlizenz auf Seite 8-3*.

Prozedur

1. Gehen Sie wie folgt vor, um PolicyServer MMC zu öffnen:

   - Doppelklicken Sie auf dem Desktop auf die Verknüpfung **PolicyServer MMC**.
   - Wechseln Sie in den Ordner, der während der Installation festgelegt wurde, und doppelklicken Sie anschließend auf `PolicyServerMMC.exe`.

   Das Authentifizierungsfenster für PolicyServer MMC wird angezeigt.



ABBILDUNG 4-2. Das Authentifizierungsfenster von PolicyServer MMC

2. Geben Sie die folgenden Parameter an:

OPTION	BEZEICHNUNG
Unternehmen	Geben Sie das Unternehmen ein.
Benutzername	Geben Sie den Benutzernamen eines Unternehmensadministratorkontos ein.

OPTION	BEZEICHNUNG
Kennwort	Geben Sie das Kennwort für den Benutzernamen ein.
Server	Geben Sie die IP-Adresse oder den Host-Namen von PolicyServer einschließlich der Portnummer ein, die dieser Konfiguration zugeordnet wurde.

3. Optional: Wenn eine Smartcard zur Authentifizierung verwendet werden soll, wählen Sie **Smartcard verwenden**.

4. Klicken Sie auf **Anmelden**.

5. Warten Sie, bis PolicyServer MMC eine Verbindung zu PolicyServer erstellt.

PolicyServer MMC wird geöffnet.

Top-Gruppe hinzufügen

Gruppen vereinfachen die Verwaltung von Endpoint Encryption Agents, Benutzern, Richtlinien, Untergruppen und Geräten. Die Top-Gruppe ist die Gruppe auf der höchsten Stufe.



Hinweis

Es ist nicht möglich, die Konten Unternehmensadministrator oder Unternehmensauthentifizierer Gruppen hinzuzufügen. Um einen Gruppenadministrator zu erstellen, fügen Sie einen Benutzer hinzu, und ändern Sie seine Kontoberechtigungen innerhalb der Gruppe. .

Prozedur

1. Klicken Sie mit der rechten Maustaste im linken Fenster auf das Unternehmen, und klicken Sie anschließend auf **Top-Gruppe hinzufügen**.

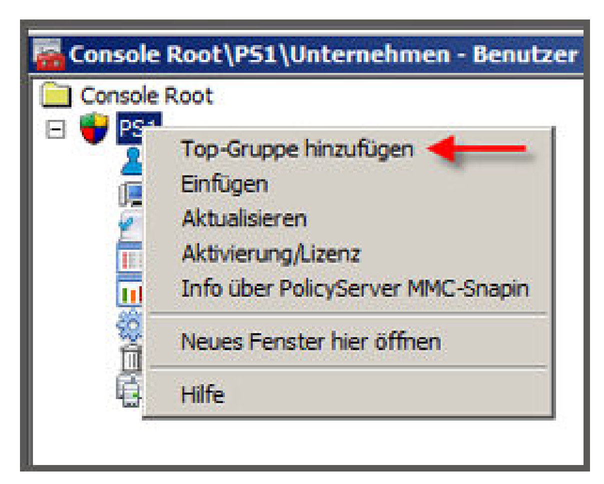


ABBILDUNG 4-3. Fenster "Top-Gruppe hinzufügen"

Das Fenster **Neue Gruppe hinzufügen** wird angezeigt.

2. Geben Sie den Namen und eine Beschreibung der Gruppe an.

3. Wenn Endpoint Encryption Geräte verwendet werden, die Unicode nicht unterstützen, wählen Sie **Altgeräte unterstützen**.



Hinweis

Einige Altgeräte sind möglicherweise nicht in der Lage, unter Verwendung von Unicode mit PolicyServer zu kommunizieren. Weisen Sie Unicode-Geräte und ältere Endpoint Encryption Geräte verschiedenen Gruppen zu.

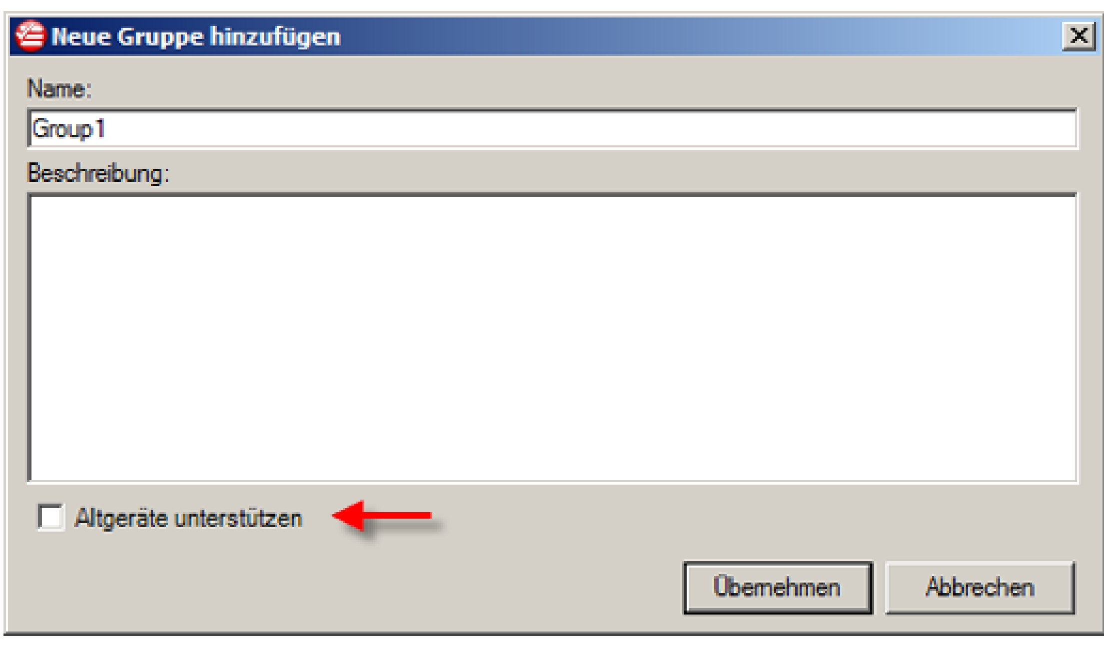


ABBILDUNG 4-4. Fenster "Neue Gruppe hinzufügen"

4. Klicken Sie auf **Übernehmen**.

5. Wenn die Bestätigungsmeldung angezeigt wird, klicken Sie auf **OK**.

   Die neue Gruppe wird zur Baumstruktur im linken Fensterbereich hinzugefügt.

Neuen Benutzer zu einer Gruppe hinzufügen



Hinweis

Beim Hinzufügen eines Benutzers zum Unternehmen wird der Benutzer keiner Gruppe zugewiesen.

Beim Hinzufügen eines Benutzers zu einer Gruppe wird der Benutzer zur Gruppe und zum Unternehmen hinzugefügt.

Prozedur

1. Erweitern Sie die Gruppe und öffnen Sie **Benutzer**.

2. Wechseln Sie in den rechten Fensterbereich, klicken Sie mit der rechten Maustaste auf einen freien Bereich, und wählen Sie anschließend **Neuen Benutzer hinzufügen**.

   Das Fenster **Neuen Benutzer hinzufügen** wird angezeigt.

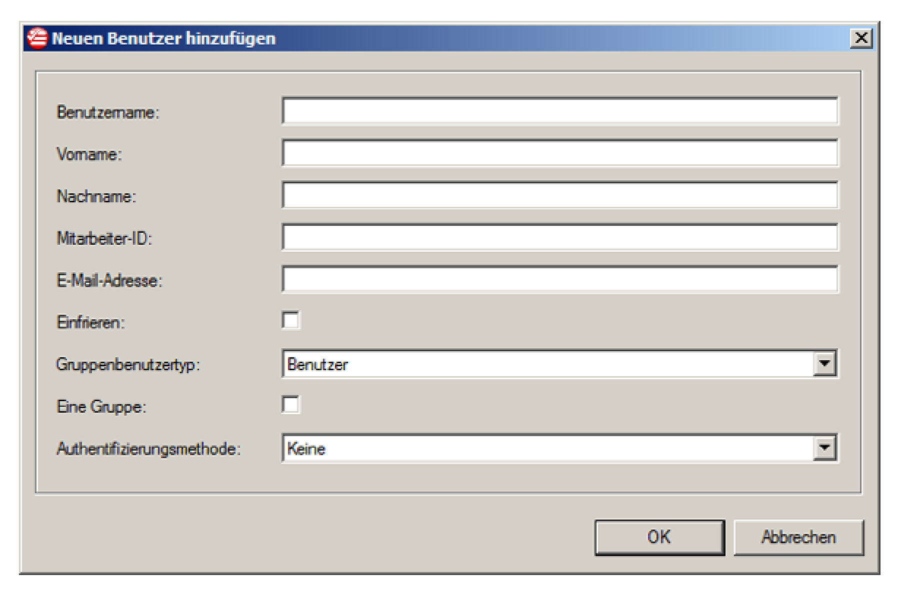


ABBILDUNG 4-5. Fenster "Neuen Benutzer hinzufügen"

3. Geben Sie die folgenden Optionen an:

OPTION	BEZEICHNUNG
Benutzername	Geben Sie den Benutzernamen für das neue Benutzerkonto an (erforderlich).
Vorname	Geben Sie den Vornamen des Benutzers für das neue Benutzerkonto an (erforderlich).

Option	Bezeichnung
Nachname	Geben Sie den Nachnamen des Benutzers für das neue Benutzerkonto an (erforderlich).
Mitarbeiter-ID	Geben Sie die Mitarbeiter-ID des Benutzers für das neue Benutzerkonto an (optional).
Einfrieren	Wählen Sie, ob das neue Benutzerkonto vorübergehend deaktiviert werden soll (optional). Wenn das Konto eingefroren ist, kann sich der Benutzer nicht an Geräten anmelden.
Gruppenbenutzertyp	Wählen Sie die Berechtigungen für das neue Konto. **Hinweis** Informationen über Kontorollen finden Sie unter *Endpoint Encryption Benutzerrollen auf Seite 1-20*. Zu den Optionen gehören: • Benutzer • Authentifizierer • Administrator **Hinweis** Es ist nicht möglich, die Konten Unternehmensadministrator oder Unternehmensauthentifizierer zu Gruppen hinzuzufügen.
Eine Gruppe	Wählen Sie, ob das neue Benutzerkonto ein Mitglied von mehreren Gruppenrichtlinien sein darf.
Authentifizierungsmethode	Wählen Sie die Methode aus, mit der sich das neue Benutzerkonto an den Endpoint Encryption Geräten anmelden wird. **Hinweis** Die Standardauthentifizierungsmethode für Benutzer lautet **Keine**.

4. Klicken Sie auf **OK**.

   Der neue Benutzer wird der ausgewählten Gruppe und zum Unternehmen hinzugefügt. Der Benutzer kann sich nun an den Endpoint Encryption Geräten anmelden.

Einem Benutzer das Installieren in eine Gruppe erlauben

Vor der Installation der Agents müssen Sie mindestens einem Benutzer in einer Gruppe die Berechtigung erteilen, Agents zu installieren.

Prozedur

1. Erweitern Sie die Gruppe, und öffnen Sie **Benutzer**.
2. Klicken Sie mit der rechten Maustaste auf das Benutzerkonto, und wählen Sie **Benutzer das Installieren in diese Gruppe erlauben** aus.

PolicyServer – Active Directory-Synchronisierung

PolicyServer unterstützt die Active Directory (AD)-Synchronisierung für eine konfigurierte PolicyServer Gruppe. Durch die Synchronisierung werden AD-Benutzer automatisch zu konfigurierten PolicyServer Gruppen hinzugefügt bzw. aus diesen entfernt.

Active Directory-Überblick

Für die PolicyServer AD-Synchronisierung sind drei Komponenten erforderlich:

1. Eine konfigurierte AD-Domäne.
2. Eine PolicyServer Gruppe, die so konfiguriert ist, dass sie auf eine gültige AD-Organisationseinheit (Organizational Unit, OU) verweist.
3. Entsprechende Anmeldedaten für den Zugriff auf die AD-Domäne, die mit dem eindeutigen Namen der PolicyServer Gruppe übereinstimmen.

Wenn die Synchronisierung ordnungsgemäß konfiguriert ist, erstellt sie automatisch neue PolicyServer Benutzer und verschiebt diese in die zugeordneten Gruppen auf dem PolicyServer. Während der Synchronisierung wird der PolicyServer aktualisiert, so dass die Benutzer und die Gruppenzuweisungen der zugeordneten Gruppen übereinstimmen.

Wenn ein neuer Benutzer zur Domäne hinzugefügt und in der Organisationseinheit platziert wird, wird dieser Benutzer markiert, so dass AD diesen Benutzer während der nächsten Synchronisierung in PolicyServer erstellt und anschließend in die zugeordnete PolicyServer Gruppe verschiebt.

Wenn ein Benutzer aus AD gelöscht wird, wird er automatisch aus der zugeordneten PolicyServer Gruppe und dem Unternehmen entfernt.

Um Nicht-Domänenbenutzer zu Gruppen hinzuzufügen, die mit der Domäne synchronisiert werden, können Sie eindeutige Endpoint Encryption Benutzer anlegen und diese zugeordneten PolicyServer Gruppen hinzufügen. Dabei ist es nicht erforderlich, diese Benutzer über das Synchronisierungssystem zu ändern.

Wenn Sie den Endpoint Encryption Benutzer aus einer zugeordneten Gruppe in PolicyServer entfernen, wird dieser Domänenbenutzer nicht automatisch vom Synchronisierungssystem wieder hinzugefügt. Dies verhindert das Überschreiben Ihrer Aktion für diesen Endpoint Encryption Benutzer. Wenn Sie einen synchronisierten Domänenbenutzer manuell wieder in eine zugeordnete Gruppe verschieben, beginnt das Synchronisierungssystem automatisch wieder damit, den Benutzer in der Gruppe zu verwalten.

Active Directory konfigurieren

Für diese Aufgabe wird vorausgesetzt, dass der Domänencontroller auf Windows Server 2003 eingerichtet wurde und AD installiert ist.

Prozedur

1. Navigieren Sie zu **Start** > **Programme** > **Verwaltung** > **Active Directory-Benutzer und -Computer**.

   Das Fenster "Active Directory-Benutzer und -Computer" wird geöffnet.

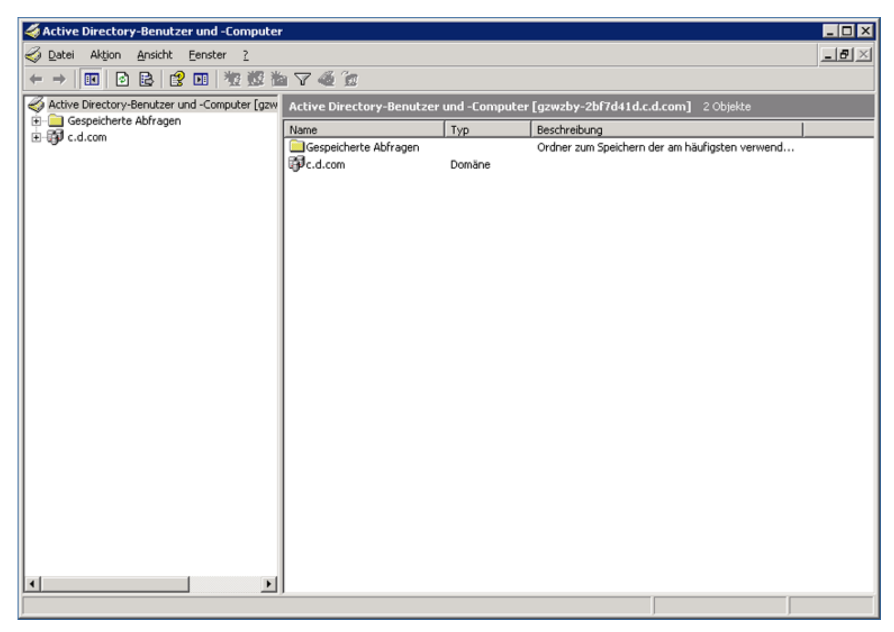


ABBILDUNG 4-6. Active Directory-Benutzer und -Computer

2. Klicken Sie mit der rechten Maustaste auf die neue Domäne, die bei der Installation von AD erstellt wurde, und wählen Sie **Neu** aus.

3. Wählen Sie **Organisationseinheit** aus.

4. Klicken Sie auf **Weiter**.

5. Geben Sie im Fenster **Neues Objekt - Organisationseinheit** den neuen Namen an und klicken Sie auf **OK**.

   Die neue Gruppe wird in der linken Navigation unter der Domäne angezeigt.

   Die neue Gruppe wird zur Synchronisierung mit einer PolicyServer Gruppe verwendet. Zunächst müssen jedoch Benutzer zur Gruppe hinzugefügt werden.

6. Klicken Sie mit der rechten Maustaste auf die neue Gruppe und wählen Sie **Neuer Benutzer** aus.

7. Geben Sie im Fenster **Neues Objekt - Benutzer** die Kontoinformationen des neuen Benutzers an und klicken Sie auf **Weiter**.

8. Geben Sie das Domänenkennwort des neuen Benutzers an, und bestätigen Sie es. Klicken Sie auf **Weiter**, um fortzufahren.



Hinweis

Deaktivieren Sie die Option **Benutzer muss Kennwort bei nächster Anmeldung ändern** und aktivieren Sie die Option **Kennwort läuft nie ab**, um weitere Tests zu einem späteren Zeitpunkt zu vereinfachen.

9. Wenn die Installation abgeschlossen ist, klicken Sie auf **Fertig stellen**.

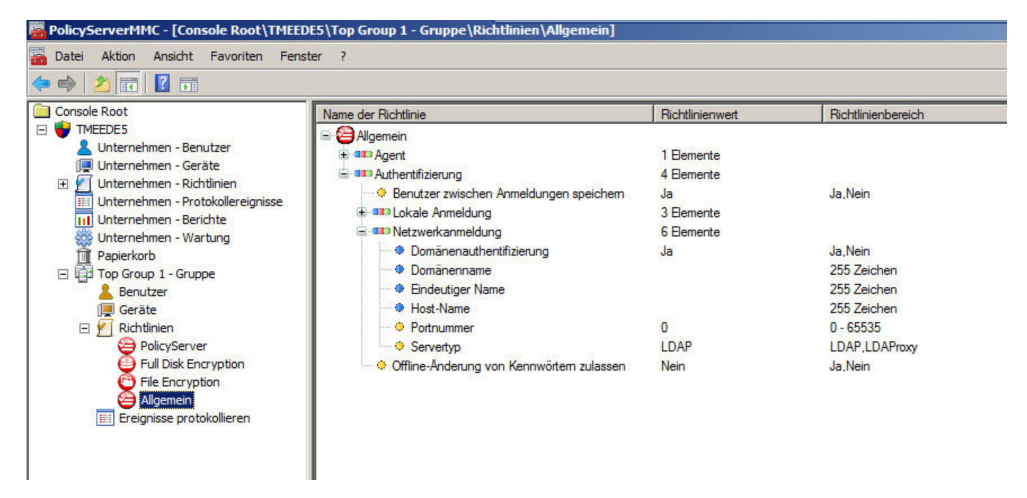
   Der Domänencontroller ist mit einer neuen Organisationseinheit und einem Benutzer in dieser Gruppe konfiguriert. Um diese Gruppe mit PolicyServer zu synchronisieren, installieren Sie PolicyServer, und erstellen Sie eine Gruppe für die Synchronisierung. Für den nächsten Abschnitt wird vorausgesetzt, dass PolicyServer bereits installiert ist.

10. Melden Sie sich bei PolicyServer MMC an.

11. Klicken Sie mit der rechten Maustaste auf das Unternehmen, und wählen Sie **Top-Gruppe hinzufügen**.

12. Geben Sie den Namen und die Beschreibung für die Gruppe an und klicken Sie anschließend auf **Anwenden**.

13. Um die Synchronisierungsrichtlinie zu konfigurieren, öffnen Sie die Gruppe und navigieren Sie zu **Allgemein** > **Authentifizierung** > **Netzwerkanmeldung**.



14. Öffnen Sie **Eindeutiger Name**, und geben Sie den vollständig qualifizierten eindeutigen Namen aus der konfigurierten AD-Organisation an, die mit dieser Gruppe synchronisiert werden soll. Klicken Sie anschließend auf **OK**.



Hinweis

Das Format für den eindeutigen Namen einer Organisationseinheit namens "Engineering" auf der Domäne "test.home" ist:
`OU=Engineering,DC=TEST,DC=HOME`

---

15. Öffnen Sie **Domänenname**, und geben Sie den NetBIOS-Domänennamen an, der zum Konfigurieren des AD-Servers verwendet wurde.

    Nachdem die PolicyServer Richtlinie konfiguriert wurde, ist als letzter Konfigurationsvorgang die Erstellung der Synchronisierungskonfiguration über das AD Synchronization Configuration Tool erforderlich. Mit diesem Tool können Sie für jede synchronisierte Organisationseinheit und jeden Domänencontroller separate AD-Anmeldedaten erstellen.

16. Um auf das **AC Synchronization Configuration** Tool zuzugreifen, navigieren Sie zum Installationsordner von PolicyServer und öffnen Sie **ADSyncConfiguration.exe**.

Das Fenster "PolicyServer - AD Synchronization Tool" wird geöffnet.

PolicyServer - Active Directory-Synchronisierung

Informationen zum Unternehmen

Stellen Sie sicher, dass Active Directory und PolicyServer verfügbar und für Active Directory konfiguriert sind, um die Synchronisierung für alle konfigurierten Gruppen zu ermöglichen.

Eindeutiger Gruppenname	Letzte Synchronisierung

Löschen Hinzufügen

Beenden

17. Klicken Sie auf **Add**, um die Anmeldedaten für die AD-Organisationseinheit anzugeben.



Hinweis

Für Server, die zusätzliche Anmeldedaten erfordern, können die Benutzer den entsprechenden Administrator-Benutzernamen und das Administrator-Kennwort eingeben, um über dieses Tool eine Verbindung zum Domänencontroller herzustellen.

18. Beenden Sie das **ADSyncConfiguration** Tool.

Die Synchronisierung zwischen dem AD und PolicyServer ist abgeschlossen. Die Synchronisierung erfolgt automatisch alle 45 Minuten (dies ist das standardmäßig von Microsoft Domänencontrollern verwendete Synchronisierungsintervall). Sie können eine Synchronisierung erzwingen, indem Sie den PolicyServer Windows-Dienst anhalten und neu starten. Die Domänensynchronisierung wird kurz nach dem Start des PolicyServer Windows-Dienstes und anschließend alle 45 Minuten ausgeführt.

LDAP-Proxy

Die optionale Funktion LDAP-Proxy ermöglicht die Domänenauthentifizierung bzw. das Single Sign-On (SSO) über einen externen Proxy-Server in der DMZ (Demilitarisierte Zone) des Kunden.



Hinweis

- Die LDAP-Proxy-Installation ist in gehosteten Umgebungen, die Domänenauthentifizierung/Single-Sign-On (SSO) verwenden, erforderlich.
- LDAP-Proxy-Versionen vor 3.1 werden nicht mehr unterstützt.
- Kunden, die eine ältere LDAP-Proxy-Version verwenden, müssen zuerst ein Upgrade auf Version 3.1 durchführen.

LDAP-Voraussetzungen

TABELLE 4-2. Hardware- und Softwarespezifikationen für LDAP

SPEZIFIKATION	VORAUSSETZUNG
Prozessor	Intel™ Core™ 2 oder kompatibler Prozessor.
Arbeitsspeicher	• Mindestens: 2GB
Festplattenspeicher	• Mindestens: 30GB • Erforderlich: 20% verfügbaren Festplattenspeicher

<table>
<tr><th>SPEZIFIKATION</th><th>VORAUSSETZUNG</th></tr>
<tr><td>Netzwerkverbindung</td><td>• Der Server muss sich in der Domäne befinden und Zugriff auf AD haben.
• Die Serveradresse muss über das Internet zugänglich sein.
• Eingehende Proxy-Verbindungen müssen zugelassen werden.
• PolicyServer muss Zugriff auf den IIS-Server dieses Servers haben.</td></tr>
<tr><td>Betriebssystem</td><td>• Windows Server 2008 / 2008 R2 64 Bit</td></tr>
<tr><td>Anwendungen und Einstellungen</td><td>• Anwendungsserverrolle
  • IIS
  • ASP (Active Server Pages) zulassen
  • ASP.NET zulassen
• Microsoft .Net Framework 2.0 SP2</td></tr>
</table>

Checkliste für LDAP-Proxy-Hardware

TABELLE 4-3. Checkliste für LDAP-Proxy-Hardware

LDAP-PROXY-SERVER		ANMERKUNGEN
Angaben zu Windows Server	Betriebssystemversion	
	Service-Pack-Version	
Angaben zur Hardware	Marke	
	RAM	
	Modell	
	CPU	

LDAP-PROXY-SERVER		ANMERKUNGEN
Installierte Software auf dem Server	IIS	
	Microsoft .NET SP 2.0 Sp1 oder höher	
Angaben zum Netzwerk	IP-Adresse	
	Subnetzmaske	
	Host-Name	
	Domänenname	
	Verfügbare Anmeldedaten der Domäne (nur für SSO)	

Services auf mehreren Endpunkten konfigurieren

Um eine 3-Stufen-Netzwerktopographie zu erstellen, können Sie die Dienste gesondert auf einen Endpunkt verteilen, der sich in der Netzwerk-DMZ befindet. Dadurch können Sie PolicyServer sicher hinter der Firewall konfigurieren. Sie können Client Web Proxy auf dem gesonderten Endpunkt installieren, damit dieser als Proxy den Datenverkehr entweder weiterleitet oder weiterleitet und filtert. Client Web Proxy verwaltet die folgenden Dienste:

Traffic Forwarding Service

Mit Traffic Forwarding Service leiten Sie den gesamten Datenverkehr von Endpoint Encryption 5.0 Patch 1 Agents zum verbundenen PolicyServer weiter. Der Dienst kommuniziert mit dem Endpoint Encryption Dienst auf dem betreffenden PolicyServer.

Client-Web-Service

Mit Client-Web-Service leiten Sie den gesamten Datenverkehr von älteren Endpoint Encryption (3.1.3 und niedriger) zum verbundenen PolicyServer weiter. Der Dienst kommuniziert mit dem PolicyServer Windows-Dienst auf dem betreffenden PolicyServer. Neben der Weiterleitung wird der Datenverkehr auch von Client-Web-Service gefiltert, um Sicherheitsbedrohungen zu verhindern.

Weitere Informationen zu Diensten finden Sie unter *Info über PolicyServer auf Seite 1-13*.

Info über Traffic Forwarding Service

Sie können Traffic Forwarding Service in Umgebungen einsetzen, in denen sich Endpoint Encryption 5.0 Patch 1 Agents und PolicyServer in f verschiedenen lokalen Netzwerken befinden. Endpoint Encryption 5.0 Patch 1 Agents kommunizieren über RESTful. Traffic Forwarding Service befindet sich zwischen den Agents und PolicyServer, um den unsicheren Zugriff auf Richtlinien zu verhindern. Das Installationsprogramm von Traffic Forwarding Service konfiguriert den TMEEservice-Dienst. Dabei handelt es sich um denselben RESTful-Dienst, der vom PolicyServer Installationsprogramm in Umgebungen installiert wird, die keinen Proxy-Server einsetzen.



Hinweis

- Es ist nicht möglich, Traffic Forwarding Service und PolicyServer auf demselben Endpunkt zu installieren.
- Der Standardwert ist 8080.

Info über Client-Web-Service

Sie können Client-Web-Service in Umgebungen einsetzen, in denen sich ältere Endpoint Encryption Agents (3.1.3 und älter) befinden und PolicyServer in anderen lokalen Netzwerken installiert wurde. Ältere Endpoint Encryption Agents kommunizieren mit Hilfe von SOAP. Client-Web-Service befindet sich zwischen den älteren Endpoint Encryption Agents und dem PolicyServer Windows-Dienst, um einen unsicheren Richtlinienzugriff zu verhindern. Das Installationsprogramm des Client-Web-Service konfiguriert MAWebService2 (Legacy Web Service). Dabei handelt es sich um denselben Microsoft IIS-Dienst, der vom PolicyServer Installationsprogramm in Umgebungen installiert wird, die keinen Proxy-Server einsetzen.



Hinweis

- Es ist nicht möglich, Client-Web-Service und PolicyServer auf demselben Endpunkt zu installieren.
- Der Standard-Port für Agents von Endpoint Encryption 3.1.3 oder niedriger ist 8080.
- In Umgebungen, in denen sowohl neue als auch ältere Versionen von Endpoint Encryption ausgeführt werden, sollten Sie für jeden Proxy-Dienst, der mit PolicyServer kommuniziert, andere Ports konfigurieren.

Client Web Proxy konfigurieren



Hinweis

Sorgen Sie dafür, dass PolicyServer auf einem anderen Endpunkt installiert wird.

Prozedur

1. Kopieren Sie den Installationsordner von PolicyServer auf die lokale Festplatte.
2. Öffnen Sie den Ordner **Tools**, und führen Sie `TMEEProxyInstaller.exe` aus.

   Das Begrüßungsfenster wird angezeigt.
3. Klicken Sie auf **Fortfahren**.

   Der Endpunkt wird vom Installationsprogramm von Client Web Proxy analysiert.
4. Geben Sie die IP-Adresse oder den Host-Namen von PolicyServer und die Portnummer des Endpoint Encryption Dienstes auf dem Ziel-PolicyServer an.

   Hinweis

   Die Standardeinstellung lautet `localhost:8080`.
5. Klicken Sie auf **Fortfahren**.

   Die Installation beginnt.
6. Warten Sie, bis Client Web Proxy installiert wurde.

7. Klicken Sie auf **Fertig stellen**.

8. Verifizieren Sie die Installation von Client Web Proxy.

    a. Navigieren Sie zu **Start** > **Verwaltung** > **Internetinformationsdienste-Manager**.

        Das Fenster **Internetinformationsdienste-Manager** wird angezeigt.

    b. Suchen Sie den Speicherort für die zuvor konfigurierte Site.

    c. Vergewissern Sie sich, dass **MAWebService2** konfiguriert wurde.

9. Überprüfen Sie die Installation von "Traffic Forwarding Service".

    a. Navigieren Sie zu **Start** > **Verwaltung** > **Dienste**.

        Das Fenster **Dienste** wird angezeigt.

    b. Vergewissern Sie sich, dass der Dienst **TMEEForward** gestartet wurde.

Traffic Forwarding Service ist installiert.

Upgrade

Um Zugriff auf neue Produktfunktionen zu erhalten oder eine ältere Agent-Software zu aktualisieren, um die Endpunktsicherheit zu verbessern, müssen Administratoren möglicherweise den Endpoint Encryption PolicyServer und alle verwalteten Endpunkte aktualisieren, auf denen ein Endpoint Encryption Agent ausgeführt wird. Um die Synchronisierung der Richtlinien und die Sicherheit der Informationen zu gewährleisten, müssen Sie PolicyServer immer vor den Endpoint Encryption Agents aktualisieren.

In diesem Abschnitt wird beschrieben, wie auf sichere Weise ein Upgrade von Endpoint Encryption, einschließlich PolicyServer, PolicyServer MMC und der Software für den Endpoint Encryption Agent, auf die neuesten Versionen durchgeführt werden kann. Weitere Informationen finden Sie unter *Zusammenfassung der Vorgänge zu Upgrades auf Seite 3-26*



Warnung!

Stellen Sie vor der Aktualisierung des Agent sicher, dass PolicyServer zuerst auf Version 5.0 Patch 1 aktualisiert wird. Endpoint Encryption 5.0 Patch 1 Agents können nicht mit PolicyServer 3.1.3 oder früher kommunizieren.

Upgrade-Pfade

In der folgenden Tabelle werden die Upgrade-Pfade von jeder früheren Produktversion bis Version 5.0 Patch 1 beschrieben. Einige ältere Versionen können nicht direkt auf 5.0 Patch 1 aktualisiert, sondern müssen zunächst auf eine neuere Version des Produkts aktualisiert werden. Informationen zur Installation von älteren Versionen von Endpoint Encryption finden Sie in der Dokumentation, die Sie unter folgender Adresse herunterladen können:

http://docs.trendmicro.com/de-de/enterprise/endpoint-encryption.aspx.

TABELLE 4-4. Upgrade-Pfade

PRODUKT/AGENT	VERSION	UPGRADE-PFAD
PolicyServer	3.1.3 SP1	3.1.3 SP1 → 5.0
	3.1.3	3.1.3 → 5.0
	3.1.2	3.1.2 → 5.0
Full Disk Encryption	3.1.3 SP1	3.1.3 SP1 → 5.0
	3.1.3	3.1.3 → 5.0
MobileArmor Full Disk Encryption	3.1.2	3.1.2 → Full Disk Encryption 5.0
	SP7g	SP7g → 3.1.3 → Full Disk Encryption 5.0
	SP7-SP7f	SP7-SP7f → SP7g → 3.1.3 → Full Disk Encryption 5.0
DriveArmor	3.0	Nicht unterstützt

PRODUKT/AGENT	VERSION	UPGRADE-PFAD
FileArmor	3.1.3 SP1	FileArmor 3.1.3 SP1 → File Encryption 5.0
	3.1.3	FileArmor 3.1.3 → File Encryption 5.0
	3.0.14	FileArmor 3.0.14 → FileArmor 3.1.3 → File Encryption 5.0
	3.0.13	FileArmor 3.0.13 → FileArmor 3.1.3 → File Encryption 5.0
KeyArmor	3.0.2	Es gibt keine KeyArmor 5.0 Version.
	3.0.1	

Unterstützte Agent-Versionen

Obwohl PolicyServer die Richtlinienverwaltung für alle Agents unterstützt, können sich ältere Agents nicht als neues Gerät bei PolicyServer 5.0 Patch 1 oder Control Manager registrieren. In der folgenden Tabelle wird erklärt, welche ältere Versionen als neues Gerät hinzugefügt werden können. Trend Micro empfiehlt die Verwendung der neuesten Versionen für alle Agents.

TABELLE 4-5. Unterstützte ältere Agents für neue Geräte

AGENT	VERSION	KANN ALS NEUES GERÄT REGISTRIERT WERDEN	UNTERSTÜTZE RICHTLINIEN
Full Disk Encryption	5.0	●	●
	3.1.3 SP1	●	●
	3.1.3	●	●
MobileArmor Full Disk Encryption	3.1.2		●
	SP7g		●

Agent	Version	Kann als neues Gerät registriert werden	Unterstütze Richtlinien
DriveArmor	3.0		●*
File Encryption	5.0 Patch 1	●	●
FileArmor	3.1.3	●	●
	3.0.14		●
	3.0.13		●
KeyArmor	Alle		●*


Hinweis

*Wird nur auf PolicyServer Upgrades von Endpoint Encryption 3.1.2 oder 3.1.3 unterstützt.

Upgrade von PolicyServer

Führen Sie ein Upgrade von PolicyServer durch, um Zugriff auf die Serververbesserungen und neuen Funktionen zu erhalten, die in der neusten Produktversion verfügbar sind. Während des Upgrades werden die PolicyServer Dienste vorübergehend angehalten. Es kommt jedoch zu keiner Unterbrechung beim Zugang zu den Endpoint Encryption Geräten. Vorhandene Richtlinienkonfigurationen werden beibehalten.


Hinweis

Informationen zu Neuinstallationen finden Sie unter *PolicyServer installieren auf Seite 4-3*.

Informationen zur Architektur finden Sie unter *Komponenten von Endpoint Encryption auf Seite 1-10*. PolicyServer MMC kann optional gleichzeitig installiert werden.



Warnung!

Aus Sicherheitsgründen können ältere Endpoint Encryption Agents nicht direkt mit einer PolicyServer Instanz kommunizieren, die sich in einem anderen Netzwerk befindet. Informationen zur Konfiguration eines Web-Proxys finden Sie unter *Services auf mehreren Endpunkten konfigurieren auf Seite 4-25*.

Prozedur

1. Vergewissern Sie sich, dass alle Systemvoraussetzungen erfüllt werden.

   Weitere Informationen finden Sie unter *Voraussetzungen für PolicyServer auf Seite 2-2*.

2. Führen Sie `PolicyServerInstaller.exe` aus.

   Das PolicyServer Installationsprogramm wird geöffnet.

3. Lesen Sie im Fenster **Rechtliche Hinweise zum Produkt** die Lizenzvereinbarung, und akzeptieren Sie die Bedingungen, indem Sie auf **Zustimmen** klicken.

4. Überprüfen Sie die PolicyServer Version und klicken Sie anschließend auf **Upgrade**.

   Stellen Sie sicher, dass Sie dem korrekten Upgrade-Pfad für PolicyServer folgen. Weitere Informationen finden Sie unter *Upgrade-Pfade auf Seite 3-24*.

5. Wenn die Meldung **Lizenzregistrierung** angezeigt wird, klicken Sie auf **OK**, um fortzufahren.

6. Klicken Sie im Fenster **Anmeldung beim Windows-Dienst** auf **Fortfahren**. Die Standardeinstellungen eignen sich für die meisten Umgebungen.

7. Geben Sie im Fenster **Datenbankadministrator-Anmeldung** die folgenden Informationen in den Abschnitt **Primäre Datenbank** ein:

OPTION	BEZEICHNUNG
Server	Host-Name (localhost) oder die IP-Adresse von Microsoft SQL Server.

OPTION	BEZEICHNUNG
Benutzername	Der Benutzername mit der Rolle **sysadmin** für den angegebenen Microsoft SQL Server.
Kennwort	Das Kennwort für das Konto **sysadmin**.



Hinweis

Bei Umgebungen mit mehreren SQL Server-Instanzen fügen Sie die SQL-Instanz ans Ende des PolicyServer Hostnamens oder die verwendete IP-Adresse an. Verwenden Sie zur Angabe einer Instanz die folgende Syntax:

```
<Host-Name oder IP-Adresse>\<Datenbankinstanz>
```

Das Installationsprogramm überprüft die Datenbankverbindung.

8. Gehen Sie wie folgt vor, wenn die Meldung **PolicyServer Frage** angezeigt wird:

   - Klicken Sie auf **Ja**, um die bestehenden Daten zu sichern
   - Klicken Sie auf **Nein**, um die bestehenden Daten zu überschreiben

9. Geben Sie im Fenster **Endpoint Encryption Dienst** die folgenden Parameter ein:

OPTION	BEZEICHNUNG
Portnummer	Geben Sie die Portnummer an, die PolicyServer MMC, Control Manager und Endpoint Encryption 5.0 Patch 1 Agents zur Kommunikation mit PolicyServer verwenden (Standard: 8080). **Hinweis** In Umgebungen mit älteren Agents empfiehlt Trend Micro die Verwendung von Port 8080 für den Admin-Web-Dienst und Port 80 für den Client-Web-Service. Die Portnummer muss eine positive Ganzzahl zwischen 1 und 65535 sein.
Automatisch ein neues selbstsigniertes	Wählen Sie diese Option, wenn kein Zertifikat verfügbar ist. Das Installationsprogramm generiert ein Zertifikat für die Kommunikation.

Option	Bezeichnung
Zertifikat generieren	
Ein vorhandenes Zertifikat angeben	Wählen Sie diese Option, um ein bestimmtes Zertifikat zu verwenden. Es gibt keine Einschränkungen oder Voraussetzungen für die Angabe eines vorhandenen Zertifikats, außer dass das Zertifikat korrekt formatiert ist.



Hinweis

Der Endpoint Encryption Dienst verwendet eine Web-API (RESTful) zur Authentifizierung von Agents, die eine Verbindung mit PolicyServer erstellen.

10. Wählen Sie im Fenster **Legacy-Agent-Service** den Speicherort, den die älteren Endpoint Encryption Agents (Version 3.1.3 und niedriger) zur Kommunikation mit PolicyServer nutzen, und klicken Sie anschließend auf **Fortfahren**.

11. Klicken Sie auf **Ja**, um PolicyServer MMC zu installieren.



Warnung!

Das PolicyServer Installationsprogramm kann automatisch eine Version von PolicyServer MMC installieren, die die Verwaltung des Produkts unterstützt. PolicyServer 5.0 Patch 1 unterstützt keine älteren Versionen von PolicyServer MMC. Klicken Sie nur auf **Nein**, wenn ein anderer Endpunkt mit PolicyServer MMC 5.0 Patch 1 zur Verwaltung von PolicyServer installiert ist.

Der Installationsvorgang wird gestartet.

12. Klicken Sie in der **PolicyServer Installation**-Meldung auf **OK**.

13. Klicken Sie auf **Beendet**.

14. Klicken Sie im Fenster des PolicyServer Installationsprogramms auf **Beenden**.

15. Starten Sie den Server neu.

Upgrades für mehrere PolicyServer Dienste installieren, die mit derselben Datenbank verbunden sind

Nur ein PolicyServer kann das Datenbank-Upgrade gleichzeitig durchführen.

Prozedur

1. Halten Sie den PolicyServer Windows-Dienst auf allen PolicyServer Instanzen an, außer der einen, auf die das Upgrade aufgespielt werden soll.

   a. Navigieren Sie zu **Start** > **Verwaltung** > **Dienste**.

   b. Klicken Sie mit der rechten Maustaste auf **PolicyServer Windows-Dienst**, und wählen Sie anschließend **Beenden**.

2. Führen Sie das Upgrade auf dem aktiven Server durch.

   Weitere Informationen finden Sie unter *Upgrade von PolicyServer auf Seite 4-31*.

3. Nachdem das Upgrade abgeschlossen und die Datenbank repliziert ist, führen Sie das Upgrade auf den anderen PolicyServer Instanzen durch.

Upgrade von PolicyServer MMC



Hinweis

Aus Gründen der höheren Sicherheit kann PolicyServer 5.0 Patch 1 nicht von älteren Versionen von PolicyServer MMC verwaltet werden. Sie müssen das Upgrade für PolicyServer MMC installieren.

Prozedur

1. Führen Sie *PolicyServer MMC deinstallieren auf Seite 4-36* durch.

2. Führen Sie *PolicyServer MMC installieren auf Seite 4-9* durch.

Auf Control Manager migrieren

Administratoren können Endpoint Encryption nur mit PolicyServer MMC verwalten, oder sie verwalten Endpoint Encryption mit Control Manager zur Verwaltung von Richtlinien, Benutzern und Geräten und setzen PolicyServer MMC für die erweiterte Protokollverwaltung und Berichterstellung ein.Weitere Informationen finden Sie unter *Integration des Control Managers auf Seite 5-1*.

Deinstallation

Im folgenden Abschnitt wird die Deinstallation von PolicyServer erläutert. Ein häufiger Anwendungsfall zur Deinstallation von PolicyServer sind falsche Informationen, die bei der Installation von PolicyServer angegeben wurden.

PolicyServer MMC deinstallieren

Deinstallieren Sie den Agent mit der Windows-Funktion **Programme und Features**. den PolicyServer MMC.



Hinweis

Die Deinstallation von PolicyServer MMC wirkt sich nicht auf die PolicyServer Datenbank und Dienste aus.

Prozedur

1. Navigieren Sie zu **Start** > **Einstellungen** > **Systemsteuerung** > **Programme und Features**

   Das Fenster **Programme und Features** wird angezeigt.

2. Wählen Sie PolicyServer aus der Liste der installierten Programme.

3. Klicken Sie auf **Entfernen**.

4. Wenn die Meldung **Programme hinzufügen oder entfernen** angezeigt wird, klicken Sie zur Bestätigung auf **Ja**.

Die Deinstallation ist abgeschlossen, wenn das Programm aus der Liste entfernt wurde.

PolicyServer deinstallieren

Bei der Deinstallation von PolicyServer werden alle Endpoint Encryption Dienste entfernt. Die Deinstallation von PolicyServer wirkt sich nicht auf die Endpoint Encryption Datenbank aus.



Warnung!

Obwohl sich die Deinstallation von PolicyServer nicht auf die Endpoint Encryption Datenbank auswirkt, werden bei der Deinstallation von PolicyServer alle Endpoint Encryption Dienste entfernt. Endpoint Encryption Benutzer können sich erst wieder bei den Endpoint Encryption Geräten anmelden, nachdem PolicyServer wieder installiert wurde.

Prozedur

1. Führen Sie `PolicyServerInstaller.exe` aus.

   Das PolicyServer Installationsprogramm wird geöffnet.

2. Lesen Sie im Fenster **Rechtliche Hinweise zum Produkt** die Lizenzvereinbarung, und akzeptieren Sie die Bedingungen, indem Sie auf **Zustimmen** klicken.

3. Klicken Sie im Fenster **PolicyServer Dienste** links auf **Deinstallieren**.

   Die Deinstallation von PolicyServer beginnt.

4. Warten Sie, bis im Rahmen der Deinstallation von PolicyServer alle Dienste und Datenbankeinstellungen entfernt wurden.

5. Klicken Sie auf **Beendet**.

6. Starten Sie den Server neu.

7. Optional können Sie PolicyServer erneut installieren.

   Weitere Informationen finden Sie unter *PolicyServer installieren auf Seite 4-3*.



Kapitel 5

Integration des Control Managers

In diesem Kapitel wird erklärt, wie Sie Endpoint Encryption und Trend Micro Control Manager integrieren. Sie können PolicyServer mit Control Manager anstelle von PolicyServer MMC verwalten.



Hinweis

Informationen über die verfügbaren Management-Konsolen zur Steuerung der Implementierung von Endpoint Encryption finden Sie unter *Management-Konsolen auf Seite 2-6*.

Es werden folgende Themen behandelt:

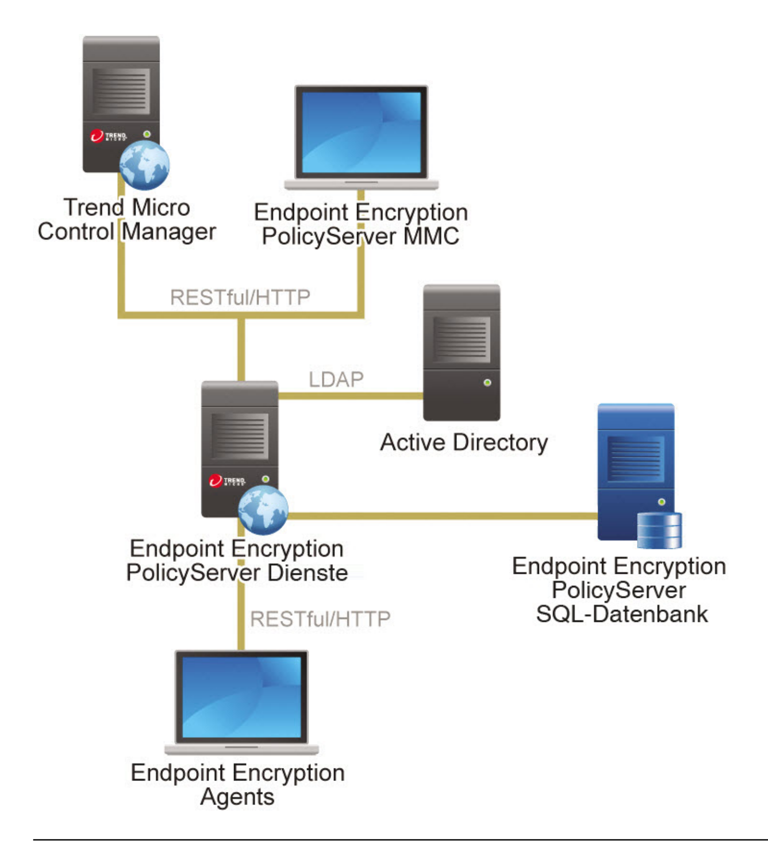
Info über Integration des Control Managers

Sie können Endpoint Encryption nur mit PolicyServer MMC flexibel verwalten, oder Sie verwalten Endpoint Encryption mit Control Manager für die Verwaltung von Richtlinien, Benutzern und Geräten und setzen PolicyServer MMC für die erweiterte Protokollverwaltung und Berichterstellung ein.

Der Trend Micro Control Manager ist eine zentrale Management-Konsole zur Verwaltung von Produkten und Services von Trend Micro auf Gateways, Mail-Servern, File-Servern und Unternehmensdesktops. Administratoren können mit den Funktionen zur Richtlinienverwaltung die Produkteinstellungen für die verwalteten Produkte und Endpunkte konfigurieren und verteilen. Die webbasierte Management-Konsole von Control Manager bietet einen zentralen Überwachungspunkt für die Verwaltung der Produkte und Dienste für Virenschutz und Content Security im gesamten Netzwerk.

Mit Control Manager kann der Systemadministrator Aktivitäten wie beispielsweise auftretende Virenausbrüche, Sicherheitsverstöße oder mögliche Viren-/Malware-Eintrittsstellen überwachen und aufzeichnen. Der Systemadministrator kann Update-Komponenten herunterladen und im Netzwerk verteilen und somit einen einheitlichen und aktuellen Schutz gewährleisten. Zu den Beispielen für Update-Komponenten zählen die Viren-Pattern-Dateien, die Scan Engine und die Anti-Spam-Regeln. Mit Control Manager sind sowohl manuelle als auch zeitgesteuerte Updates möglich. Mit Control Manager können Produkte in Gruppen oder einzeln konfiguriert und verwaltet werden.

Die folgende Darstellung illustriert, wie Sie Endpoint Encryption zum ersten Mal verteilen und Control Manager zur Verwaltung von PolicyServer verwenden. In einer Control Manager Installation setzen Administratoren Control Manager für alle Endpoint Encryption Richtlinien, Benutzer und Gerätefunktionen ein und verwenden PolicyServer MMC nur für die erweiterte Unternehmenswartung.





Hinweis

In Umgebungen, in denen Control Manager eingesetzt wird, werden Änderungen an PolicyServer Richtlinien immer von Control Manager gesteuert. Alle mit PolicyServer MMC durchgeführten Änderungen werden beim nächsten Mal überschrieben, wenn Control Manager die Richtlinien mit der PolicyServer Datenbank synchronisiert.

Auf Control Manager migrieren

Die Migration auf Control Manager erfolgt nicht automatisiert. Das folgende Verfahren beschreibt die manuelle Konfiguration von Control Manager entsprechend der bestehenden Konfiguration.

Prozedur

1. Aktualisieren Sie PolicyServer auf Version 5.0 Patch 1.

   Weitere Informationen finden Sie unter *Überlegungen zum Upgrade auf Seite 3-23*.

2. Installieren und Konfigurieren von Control Manager.

   Weitere Informationen finden Sie in der begleitenden Dokumentation:

   http://docs.trendmicro.com/en-us/enterprise/control-manager.aspx

3. Fügen Sie PolicyServer zu Control Manager hinzu.

   Weitere Informationen finden Sie unter *PolicyServer als verwaltetes Produkt zu Control Manager hinzufügen auf Seite 5-4*.

4. Fügen Sie alle vorhandenen Benutzer mit dem Widget "Endpoint Encryption Benutzer" zu Control Manager hinzu.

5. Erstellen Sie für jede derzeit vorhandene Gruppe eine neue Richtlinie.

   Weitere Informationen finden Sie unter *Eine Richtlinie erstellen auf Seite 5-8*.

6. Geben Sie in jeder neuen Richtlinie ein Richtlinienziel für jedes Gerät an, das der vorherigen Gruppe zugeordnet wurde.

   Weitere Informationen finden Sie unter *Richtlinienziele angeben auf Seite 5-9*.

7. Verteilen Sie die Richtlinien mit Control Manager.

   Weitere Informationen finden Sie unter *Eine Richtlinie erstellen auf Seite 5-8*.

PolicyServer als verwaltetes Produkt zu Control Manager hinzufügen

Endpoint Encryption ermöglicht, dass Administratoren PolicyServer mit Hilfe von Trend Micro Control Manager steuern und Endpoint Encryption Agent-Richtlinien verwalten, oder mit Trend Micro OfficeScan die Endpoint Encryption AgentSoftware auf verwaltete Endpunkte verteilen.

Wenn Sie Control Manager zur Verwaltung von PolicyServer verwenden möchten, müssen Sie PolicyServer als verwaltetes Produkt hinzufügen.

Vergewissern Sie sich bevor Sie fortfahren, dass die folgenden Aufgaben abgeschlossen wurden:

1. Installieren und Konfigurieren von Control Manager.

   Die begleitende Dokumentation finden Sie unter:

   http://docs.trendmicro.com/en-us/enterprise/control-manager.aspx

2. Installieren und Konfigurieren von PolicyServer.

Informationen zur Konfiguration weiterer Control Manager Verfahren finden Sie im *Endpoint Encryption Administratorhandbuch*.



Wichtig

Endpoint Encryption unterstützt immer nur eine einzige konfigurierte PolicyServer Instanz in Control Manager. Es ist nicht möglich, mehrere PolicyServer Konfigurationen hinzuzufügen. Wenn Sie einen anderen PolicyServer konfigurieren möchten, müssen Sie zunächst den zuvor konfigurierten PolicyServer entfernen.

Prozedur

1. Überprüfen Sie alle Systemvoraussetzungen für kompatible Produktversionen.

   Weitere Informationen finden Sie unter *Systemvoraussetzungen auf Seite 2-1*.

2. Melden Sie sich bei Control Manager an.

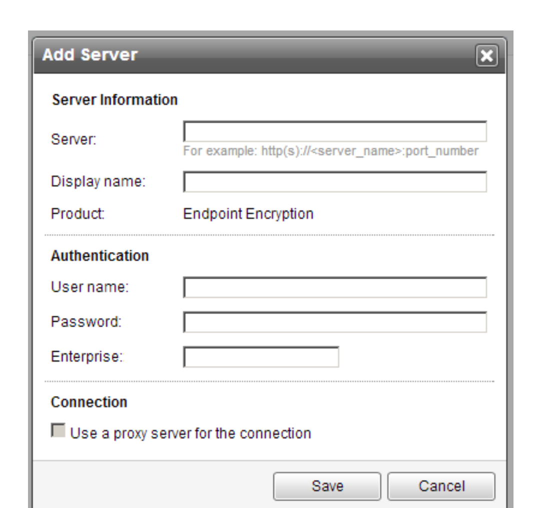
3. Navigieren Sie zu **Richtlinien** > **Richtlinienressourcen** > **Verwaltete Server**.

   Das Fenster **Verwaltete Server** wird angezeigt.

4. Wählen Sie im Listenfeld **Servertyp** die Option **Endpoint Encryption**.

5. Klicken Sie auf **Hinzufügen**.

Das Fenster **Server hinzufügen** wird angezeigt.



6. Geben Sie die Optionen für die **Serverinformationen** an.

   - **Server**: Geben Sie den Host-Namen und die Portnummer für PolicyServer an. Verwenden Sie das folgende Format:

     ```
     http(s)://<Servername>:Portnummer
     ```

     Hinweis

     Control Manager kommuniziert mit dem PolicyServer Endpoint Encryption Dienst. Die Standardportnummer lautet 8080.

   - **Anzeigename:** Geben Sie an, wie PolicyServer im Fenster **Verwaltete Server** angezeigt wird.

7. Legen Sie unter **Authentifizierung** den Benutzernamen und das Kennwort für das Endpoint Encryption Unternehmensadministratorkonto fest.

8. Wählen Sie unter **Verbindung** den Eintrag **Einen Proxy-Server für die Verbindung verwenden**, wenn PolicyServer eine Proxy-Serververbindung erfordert.

9. Klicken Sie auf **Speichern**.



Hinweis

Die Synchronisierung zwischen Control Manager und PolicyServer dauert u. U. einige Minuten.

PolicyServer wird als neues verwaltetes Produkt zu Control Manager hinzugefügt.

10. Informationen zur Konfiguration weiterer Control Manager Verfahren finden Sie im *Endpoint Encryption Administratorhandbuch*.

Gruppen für Control Manager Richtlinien konfigurieren

Control Manager vereinfacht die Richtlinienverwaltung, indem die Gruppen- und Richtlinienarchitektur von PolicyServer zusammengeführt wird. Die Synchronisierung der Gruppen- und Richtlinienarchitektur von PolicyServer mit der Richtlinienstruktur von Control Manager erfolgt nicht automatisiert. Das folgende Verfahren erklärt die wichtigsten Informationen, die Sie über die vorhandene Konfiguration in Erfahrung bringen müssen, bevor Sie die neue Konfiguration von Control Manager konfigurieren können.

Prozedur

1. Melden Sie sich bei PolicyServer MMC an.
2. Sammeln Sie folgenden Informationen:
    - Die Gesamtzahl der Gruppen, deren Namen und Untergruppen
    - Alle Benutzer, die den jeweiligen Gruppen zugeordnet sind
    - Die Richtlinienkonfiguration der jeweiligen Gruppen
3. Melden Sie sich bei Control Manager an.

4. Konfigurieren Sie für jede Gruppe in PolicyServer MMC eine neue Richtlinie, die der entsprechenden Gruppenrichtlinienkonfiguration entspricht.



Hinweis

Untergruppen werden nicht mehr unterstützt. Erstellen Sie entweder eine Richtlinie für jede Untergruppe oder erstellen Sie eine Richtlinie für die Gruppe, die sich auf die Untergruppen auswirkt.

5. Fügen Sie alle Benutzer jeder neuen Richtlinie hinzu.

6. Verteilen Sie jede Richtlinie.

Eine Richtlinie erstellen

Das folgende Verfahren erklärt, wie Sie eine Control Manager Richtlinie konfigurieren, die sich auf Endpoint Encryption Benutzer und Geräte auswirkt.



Wichtig

Wenn Sie ein Benutzerkonto der Richtlinie hinzufügen möchten, vergewissern Sie sich, dass das Benutzerkonto bereits vorhanden ist.

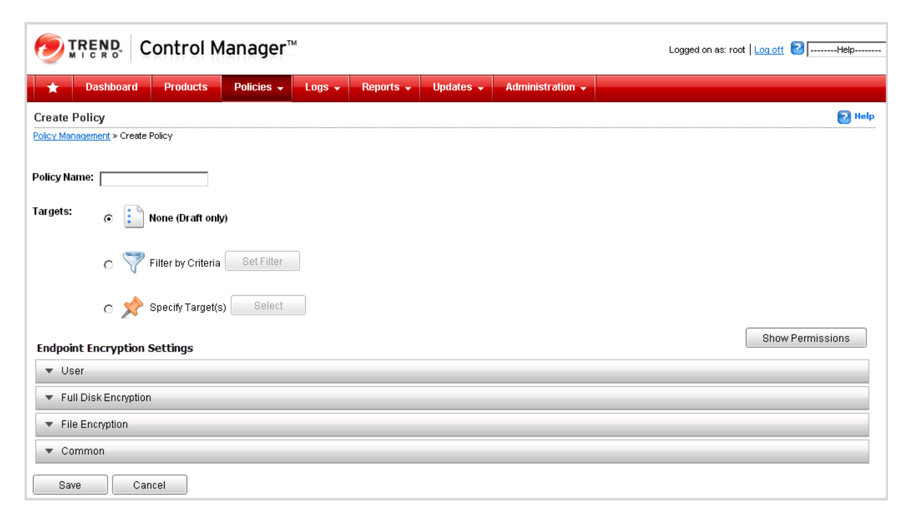
Prozedur

1. Navigieren Sie zu **Richtlinien** > **Richtlinienverwaltung**.

2. Wählen Sie im Listenfeld **Produkt** die Option **Endpoint Encryption**.

3. Klicken Sie auf **Erstellen**.

   Das Fenster **Richtlinie erstellen** wird angezeigt.



4. Geben Sie einen Richtliniennamen an.
5. Geben Sie Richtlinienoptionen an.

   Siehe *Richtlinienziele angeben auf Seite 5-9*.



Hinweis

Weitere Informationen zu den verfügbaren Richtlinienoptionen finden Sie im *Endpoint Encryption Administratorhandbuch*.

6. Klicken Sie auf **Speichern**.

Richtlinienziele angeben

Im Fenster **Ziel(e) angeben** weisen Sie die Endpoint Encryption Geräte der Richtlinie zu.



Hinweis

Das Fenster **Ziel(e) angeben** wird angezeigt, wenn Sie eine neue Richtlinie erstellen. Informationen zum Erstellen einer Richtlinie finden Sie unter *Eine Richtlinie erstellen auf Seite 5-8*.

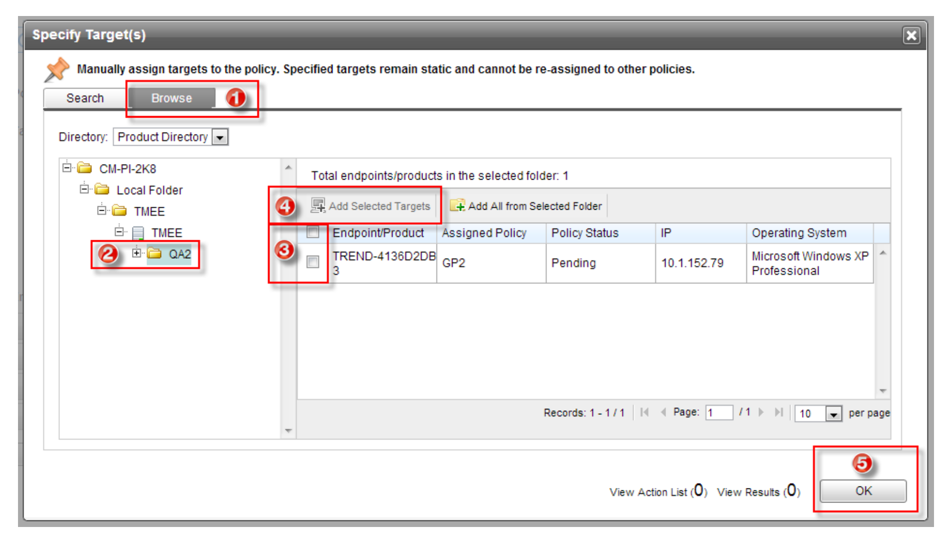


ABBILDUNG 5-1. Richtlinienziele angeben

Prozedur

1. Klicken Sie im Fenster **Ziel(e) angeben** auf die Registerkarte **Durchsuchen**.

2. Erweitern Sie die Struktur im linken Fensterbereich, um den verwalteten Ordner zu wählen.

   Beispiel: **CM-PI-2K8** > **Lokaler Ordner** > **TMEE** > **TMEE** > **QA2**

3. Wählen Sie die entsprechenden Endpoint Encryption Geräte, oder aktivieren Sie das obere Kontrollkästchen, um alle Endpoint Encryption Geräte auszuwählen, die auf der aktuellen Seite aufgelistet werden.

4. Klicken Sie auf **Ausgewählte Ziele hinzufügen**.



Hinweis

Wenn Sie sofort alle Geräte im verwalteten Ordner auswählen möchten, klicken Sie auf **Alle aus ausgewähltem Ordner hinzufügen**.

„Aktionsliste anzeigen“ und „Ergebnisse anzeigen“ werden basierend auf der Auswahl aktualisiert.

5. Klicken Sie auf **OK**.

PolicyServer in Control Manager in ein verwaltetes Produkt ändern



Wichtig

Endpoint Encryption unterstützt nur eine einzige PolicyServer Instanz in Control Manager. Es ist nicht möglich, mehrere PolicyServer Instanzen hinzuzufügen.

Prozedur

1. Sie können PolicyServer aus Control Manager entfernen.

   Weitere Informationen finden Sie unter *PolicyServer als ein verwaltetes Produkt aus Control Manager entfernen auf Seite 5-11*.

2. Sie können den neuen PolicyServer zu Control Manager hinzufügen.

   Weitere Informationen finden Sie unter *PolicyServer als verwaltetes Produkt zu Control Manager hinzufügen auf Seite 5-4*.

PolicyServer als ein verwaltetes Produkt aus Control Manager entfernen

Prozedur

1. Navigieren Sie zu **Richtlinien** > **Richtlinienressourcen** > **Verwaltete Server**.

   Das Fenster **Verwaltete Server** wird angezeigt.

2. Klicken Sie auf das Symbol **Löschen** () in der Spalte **Aktionen**.

3. Wenn die Meldung angezeigt wird, klicken Sie zur Bestätigung auf **OK**.

Die PolicyServer Instanz wird aus Control Manager entfernt. Sie können die Richtlinien mit PolicyServer MMC verwalten.



Kapitel 6

Verteilung von Endpoint Encryption Agents

Jeder Endpoint Encryption Agent hat eigene Installations- und Systemanforderungen. Erklärungen zur Konfiguration und Verwaltung finden Sie im *Endpoint Encryption Administratorhandbuch*.

Es werden folgende Themen behandelt:

Endpoint Encryption Agents

In der folgenden Tabelle werden die Endpoint Encryption Agents beschrieben, die für eine Vielzahl von Umgebungen verfügbar sind.

AGENT	BESCHREIBUNG
File Encryption	Der Endpoint Encryption Agent für die Verschlüsselung von Dateien und Ordnern auf lokalen Laufwerken und Wechselmedien. Mit File Encryption können Sie die Dateien und Ordner auf nahezu jedem Gerät, das als Laufwerk im Host-Betriebssystem angezeigt wird, schützen. Weitere Informationen finden Sie unter *Info über die File Encryption auf Seite 6-4*.
Full Disk Encryption	Der Endpoint Encryption Agent für die Verschlüsselung von Hardware und Software mit Preboot-Authentifizierung. Sie können mit Full Disk Encryption Datendateien, Anwendungen, Registrierungseinstellungen, temporäre Dateien, Auslagerungsdateien, Druck-Spooler und gelöschten Dateien auf allen Windows-Endpunkten sichern. Eine starke Preboot-Authentifizierung beschränkt den Zugriff auf das anfällige Systeme, bis der Benutzer validiert wird. Weitere Informationen finden Sie unter *Info über Full Disk Encryption auf Seite 6-3*.
Encryption Management for Microsoft BitLocker	Der Endpoint Encryption Full Disk Encryption Agent für Microsoft Windows-Umgebungen, auf denen lediglich Microsoft BitLocker auf dem Hosting-Endpunkt aktiviert werden muss. Mit dem Encryption Management for Microsoft BitLocker Agent können Sie Endpunkte mit Trend Micro Full Disk Encryption in einer bestehenden Windows-Infrastruktur sichern. Weitere Informationen finden Sie unter *Info über Full Disk Encryption auf Seite 6-3*.

AGENT	BESCHREIBUNG
Encryption Management for Apple FileVault	Der Endpoint Encryption Full Disk Encryption Agent für Mac OS-Umgebungen, auf denen lediglich Apple FileVault auf dem Hosting-Endpunkt aktiviert werden muss. Mit der Encryption Management for Apple FileVault Agent können Sie Endpunkte mit Trend Micro Full Disk Encryption in einer bestehenden Mac OS-Infrastruktur sichern. Weitere Informationen finden Sie unter *Info über Full Disk Encryption auf Seite 6-3*.



Hinweis

Endpoint Encryption 5.0 verfügt über keine KeyArmor Geräte. Es werden jedoch ältere KeyArmor Geräte unterstützt.

Info über Full Disk Encryption

Der Trend Micro Full Disk Encryption Agent kombiniert einen robusten AES256-Verschlüsselungsalgorithmus und obligatorische Authentifizierung, um Daten ohne Authentifizierung unzugänglich zu machen. Full Disk Encryption verhindert Datenverluste durch die Verschlüsselung des gesamten Laufwerks, einschließlich Betriebssystem-, Programm-, temporären und Endbenutzerdateien.

Full Disk Encryption kann flexibel eingesetzt werden und unterstützt je nach Bedarf Festplattenverschlüsselung auf Software- oder Hardwarebasis. Selbstverschlüsselnde Laufwerke vom Typ Seagate DriveTrust™, OPAL und OPAL2 werden unterstützt. Während Hardware-basierte Verschlüsselung leichter auf neuer Hardware bereitgestellt und verwaltet werden kann und eine höhere Leistungsstufe bietet, ist für die Software-basierte Verschlüsselung keine Hardware erforderlich und die Bereitstellung auf vorhandenen Endpunkten ist billiger.

Trend Micro PolicyServer steuert Richtlinien, die sich auf Full Disk Encryption auswirken. Auf diese Weise wird die komplette Endpunktsicherheit gewährleistet, die im gesamten Unternehmen zentral verwaltet wird. Full Disk Encryption ist netzwerkorientiert und aktualisiert Richtlinien, bevor die Authentifizierung zugelassen wird. Sie können Daten auf dem Endpunkt auch von einem entfernten Standort aus

sperren oder löschen, bevor auf das Betriebssystem oder auf andere vertrauliche Daten zugegriffen wird.

Trend Micro Endpoint Encryption 5.0 Patch 1 erweitert den Funktionsbereich von Full Disk Encryption, indem eine Integration mit Verschlüsselungslösungen, die zum Host-Betriebssystem gehören, durch zwei neue Endpoint Encryption Agents möglich gemacht wird:

- Encryption Management for Microsoft BitLocker
- Encryption Management for Apple FileVault

Info über die File Encryption

Der Trend Micro File Encryption Agent setzt AES-Verschlüsselung zum Schutz von Daten ein, die zwischen den Endpoint Encryption Benutzern ausgetauscht wurden bzw. die auf Wechseldatenträgern oder auf Netzwerkressourcen gespeichert sind. File Encryption kann ferner verschiedene Dateien mit unterschiedlichen Schlüsseln schützen, Sie können Zugriffsrichtlinien für den File Encryption Agent festlegen und anschließend separate Richtlinien zum Zugriff auf bestimmte Dateien anlegen. Diese Funktion ist in Umgebungen nützlich, in denen mehrere Benutzer auf denselben Endpunkt zugreifen. Verschlüsselung wird durchgeführt, nachdem die Authentifizierung stattgefunden hat.

Sie können mit Trend Micro PolicyServer angeben, welche Dateien und Ordner verschlüsselt werden sollen, sowie die Richtlinien zum Verschlüsseln der Wechseldatenträger festlegen.

Endbenutzer sind ebenfalls in der Lage, File Encryption flexibel lokal zu verwalten, indem individuelle Dateien, Ordner oder Wechseldatenträger umgehend verschlüsselt werden. Benutzer sind so in der Lage, auch auf Geschäftsreisen Daten sicher zu schützen.

Installation

Im folgenden Abschnitt werden die Voraussetzungen für Neuinstallationen von Endpoint Encryption Agents, die manuelle Installation von Endpoint Encryption Agents und die Tools zur Vorbereitung automatisierter Installationsskripts beschrieben.

Vor der Installation von Endpoint Encryption Agents

Beachten Sie Folgendes, bevor Sie die Endpoint Encryption Agents installieren:

- Vergewissern Sie sich, dass alle Systemvoraussetzungen erfüllt werden. Weitere Informationen finden Sie unter *Systemvoraussetzungen auf Seite 2-1*
- Kopieren Sie alle Agent-Installationsdateien auf die lokale Festplatte.
- Tools zum Aufbau automatisierter Installationsskripts sind verfügbar. Weitere Informationen finden Sie unter *Automatisierte Verteilungen auf Seite 6-29*
- Der Benutzer, der die Installation durchführt, benötigt lokale Administratorrechte.
- Lesen Sie *Voraussetzungen für verwaltete Endpunkte auf Seite 6-5*.

Informationen zu weiteren Überlegungen vor der Verteilung finden Sie unter *Checkliste vor der Verteilung auf Seite 3-2*.

Voraussetzungen für verwaltete Endpunkte

Nach der Installation eines beliebigen Endpoint Encryption Agent wird der Endpunkt bei PolicyServer als neues Endpoint Encryption Gerät registriert. Authentifizierung, Verschlüsselung und Remote-Aktionen des Geräts werden zentral von PolicyServer Richtlinien gesteuert. Die folgenden Voraussetzungen müssen erfüllt sein, um die verwalteten Endpunkte zu installieren:

- Der Computer hat Netzwerkzugriff und kann mit PolicyServer während der Installation kommunizieren.
- Bei Umgebungen, in denen PolicyServer MMC eingesetzt wird, wird wenigstens eine Top-Gruppe hinzugefügt.

- Bei Umgebungen, in denen Control Manager eingesetzt wird, wurde wenigstens eine Richtlinie konfiguriert.

- Der Endpoint Encryption Benutzer ist berechtigt, Geräte zur Gruppe oder Richtlinie hinzuzufügen.



Hinweis

Es ist nun möglich, mit den Rollen des Unternehmensadministrators und Unternehmensauthentifizierers die Endpoint Encryption Agents zu installieren.

- Der Benutzer, der die Installation durchführt, benötigt lokale Administratorrechte.

- Wenn Domänenauthentifizierung/Single-Sign-On aktiviert ist, muss der Benutzername mit dem Benutzernamen in Active Directory übereinstimmen. Das Active Directory-Kennwort wird zur Authentifizierung verwendet.

Automatische Verteilung von Agents

Es gibt zwei Methoden, um die Massenverteilung im Unternehmen mit einer großen Zahl an Endpunkten zu vereinfachen:

- Mit OfficeScan: *Integration von OfficeScan auf Seite 7-1*

- Sie können Installationsskripts definieren, die Sie zusammen mit Automatisierungstools wie Microsoft SCCM oder SMS einsetzen: *Automatisierte Verteilungen auf Seite 6-29*

Full Disk Encryption Verteilung

In den folgenden Abschnitten werden die Installation und Konfiguration der drei Endpoint Encryption Agents beschrieben, die Full Disk Encryption verwalten:

- Full Disk Encryption

- Encryption Management for Microsoft BitLocker

- Encryption Management for Apple FileVault



Hinweis

Es ist nun möglich, mit den Rollen des Unternehmensadministrators und Unternehmensauthentifizierers die Endpoint Encryption Agents zu installieren.

Übersicht über die Verteilung von Full Disk Encryption

Das folgende Verfahren beschreibt die Vorbereitung sowie die Installation der folgenden Full Disk Encryption Agents:

- Full Disk Encryption
- Encryption Management for Microsoft BitLocker
- Encryption Management for Apple FileVault

Prozedur

1. Nehmen Sie Änderungen am Betriebssystem vor, um den Endpunkt vorzubereiten.

   Weitere Informationen finden Sie unter *Vorbereitung von Endpunkten auf Seite 6-8*.

2. Bereiten Sie in Windows-Umgebungen die Festplatte vor.

   Weitere Informationen finden Sie unter *Die Festplatte vorbereiten auf Seite 6-10*.

3. Deaktivieren Sie während der Verteilung die Verschlüsselungsrichtlinie.

   Weitere Informationen finden Sie unter *Verschlüsselung während der Verteilung deaktivieren auf Seite 6-12*.

4. Verteilen Sie den Endpoint Encryption Agent.

   Weitere Informationen finden Sie in den folgenden Themen:

   - *Full Disk Encryption Installation auf Seite 6-12*
   - *Installation der Encryption Management for Microsoft BitLocker auf Seite 6-18*
   - *Installation der Encryption Management for Apple FileVault auf Seite 6-20*

5. Folgen Sie den Anweisungen in der Installationsaufgabe, um die Verteilung zu verifizieren.

Vorbereitung von Endpunkten

Bereiten Sie vor der Installation der Full Disk Encryption Agents den Endpunkt vor, um Datenverluste zu vermeiden. In den folgenden Themen wird erklärt, wie Sie den Endpunkt in Windows- und Mac OS-Umgebungen vorbereiten.

Windows-Endpunkt vorbereiten



Hinweis

- Sie dürfen Full Disk Encryption nicht auf Endpunkte mit mehreren Festplatten installieren. Umgebungen mit mehreren Festplatten werden nicht unterstützt.
- RAID- und SCSI-Festplatten werden nicht unterstützt.
- Full Disk Encryption für Windows 8 unterstützt keine RAID-, SCSI- oder eDrive-Laufwerke.

Prozedur

1. Trennen Sie alle USB-Speichergeräte, und schließen Sie diese erst nach der Installation des Agent und nachdem der Endpunkt neu gestartet wurde wieder an.
2. Vergewissern Sie sich, dass das Laufwerk mit dem Betriebssystem nicht bereits verschlüsselt wurde und BitLocker ausgeschaltet ist.
3. Vergewissern Sie sich, dass alle Systemvoraussetzungen erfüllt werden.

   Weitere Informationen finden Sie unter *Systemvoraussetzungen auf Seite 2-1*.
4. Ändern Sie für Endpunkte unter Windows 8, die UEFI BIOS unterstützen, die Startreihenfolge in **Legacy First**.

   a. Halten Sie in Windows 8 die UMSCHALTTASTE gedrückt und starten Sie das Gerät neu.

      Das Gerät wird neu gestartet und UEFI BIOS wird geladen.

b. Klicken Sie auf die Kachel **Problembehandlung**.

Das Fenster **Erweiterte Optionen** wird angezeigt.

c. Klicken Sie auf die Kachel **UEFI-Firmwareeinstellungen**.

Wenn die Kachel **UEFI-Firmwareeinstellungen** nicht vorhanden ist, verwendet das Gerät kein UEFI und es ist keine Änderung erforderlich.

d. Legen Sie **UEFI/Legacy Boot Priority** auf **Legacy First** fest.

e. Starten Sie den Endpunkt neu.

5. Kopieren Sie die Installationsdateien auf das Systemlaufwerk.

Den Mac OS-Endpunkt vorbereiten

Prozedur

1. Entfernen Sie alle vorhandenen Produkte zur Festplattenverschlüsselung.

2. Vergewissern Sie sich, dass die Encryption Management for Apple FileVault momentan deaktiviert ist.

a. Navigieren Sie zu **Systemeinstellungen** > **Sicherheit & Datenschutz**.

b. Wählen Sie die Registerkarte **FileVault**.



c. Klicken Sie ggf. auf das Sperrsymbol (🔒), um Änderungen vorzunehmen.

d. Geben Sie den Benutzernamen und das Kennwort für den Endpunkt ein.

e. Klicken Sie auf **FileVault deaktivieren**.

Die Festplatte vorbereiten

Full Disk Encryption verschlüsselt jeden Sektor auf dem physischen Laufwerk. Da viele Anwendungen, inkl. dem Betriebssystem, nicht den vollständigen physischen Festplattenspeicher verwenden, können Sektoren beschädigt sein. Eventuell ist auch das Laufwerk extrem fragmentiert. Die Encryption Management for Microsoft BitLocker und die Encryption Management for Apple FileVault nutzen die im Host-

Betriebssystem integrierte Verschlüsselungslösung. Wenn Sie einen dieser Endpoint Encryption Agents einsetzen, ist eine Vorbereitung der Festplatte nicht erforderlich.



Hinweis

Trend Micro empfiehlt, ein kleines Pilotprojekt mit Neuinstallationen und Upgrades durchführen, bevor der neueste Full Disk Encryption Build verteilt wird. Weitere Informationen finden Sie unter *Pilotverteilung von Endpoint Encryption auf Seite C-1*.



Wichtig

Der Full Disk Encryption Agent kann nur auf einem Endpunkt mit einem einzigen physischen Laufwerk installiert werden. Entfernen Sie alle anderen Laufwerke, bevor Sie Full Disk Encryption installieren.

Prozedur

1. Führen Sie das Defragmentierungs-Dienstprogramm von Windows auf dem Systemlaufwerk aus.

   Informationen über die Defragmentierung einer Windows-Festplatte finden Sie im folgenden Artikel:

   http://windows.microsoft.com/de-de/windows-vista/improve-performance-by-defragmenting-your-hard-disk

2. Überprüfen Sie, ob auf dem Systemlaufwerk mindestens 256MB an zusammenhängendem freiem Speicher zur Verfügung stehen.

3. Führen Sie das Dienstprogramm für die Prüfung der Datenträger-Integrität von Windows aus (erfordert einen Neustart).

   a. Rufen Sie mit einem Skript oder über eine Befehlszeile `chkdsk /f /r` auf, und planen Sie die Überprüfung der Festplatte nach dem nächsten Systemneustart.

   b. Starten Sie das Gerät neu.

   c. Tauschen Sie das Laufwerk aus, wenn `chkdsk` mehrere fehlerhafte Sektoren meldet.

4. Überprüfen Sie, ob bei der Festplatte ein normaler Master Boot Record (MBR) vorliegt, und bestätigen Sie, dass ein normaler Bootsektor auf der Bootpartition vorhanden ist. Beispiel: Auf einem Computer mit zwei bootfähigen Betriebssystemen befindet sich ein modifizierter Bootsektor.



Hinweis

GUID-Partitionstabellen (GUID Partition Table, GPT) werden momentan nicht unterstützt.

Verschlüsselung während der Verteilung deaktivieren

In der nachfolgenden Tabelle wird beschrieben, wie Sie die Verschlüsselung zentral von einer der Management-Konsolen deaktivieren. Deaktivieren Sie die Laufwerkverschlüsselung vorübergehend, um die Auswirkungen auf den Endbenutzer auf ein Minimum zu reduzieren und die Verteilung auf viele Geräte zu vereinfachen. Sobald die Gerätekompatibilität bestätigt wurde, können Sie die Verschlüsselung wahlweise wieder aktivieren.

TABELLE 6-1. PolicyServer für die Geräteverschlüsselung deaktivieren

KONSOLE	RICHTLINIENEINSTELLUNG
PolicyServer MMC	Navigieren Sie zu **Full Disk Encryption** > **PC** > **Verschlüsselung** > **Gerät verschlüsseln**, und wählen Sie **Nein**.
Control Manager	Greifen Sie auf eine neue oder vorhandene Richtlinie zu (**Richtlinien** > **Richtlinienverwaltung**), und deaktivieren Sie anschließend **Gerät verschlüsseln** unter **Full Disk Encryption**.

Full Disk Encryption Installation

Sie können mit Full Disk Encryption Datendateien, Anwendungen, Registrierungseinstellungen, temporäre Dateien, Auslagerungsdateien, Druck-Spooler und gelöschten Dateien auf allen Windows-Endpunkten sichern. Eine starke Preboot-Authentifizierung beschränkt den Zugriff auf das anfällige Systeme, bis der Benutzer validiert wird.



Hinweis

Lesen Sie das folgende Thema, bevor Sie fortfahren:

- *Systemvoraussetzungen auf Seite 2-1*
- *Vor der Installation von Endpoint Encryption Agents auf Seite 6-5*
- *Voraussetzungen für verwaltete Endpunkte auf Seite 6-5*
- *Automatisierte Verteilungen auf Seite 6-29*

Installationsvoraussetzungen für Full Disk Encryption

Das Installationsprogramm von Full Disk Encryption überprüft automatisch das Zielsystem, um sicherzustellen, dass alle erforderlichen Systemvoraussetzungen vor der Installation des Agent erfüllt sind. Beim Erkennen einer Systeminkompatibiltität wird das Installationsprogramm geschlossen und am selben Speicherort wie das Installationsprogramm wird der Text `PreInstallCheckReport.txt` generiert.

Ermitteln Sie anhand der Installations-Checkliste, welche Systemvoraussetzungen nicht erfüllt werden. Die Checkliste befindet sich im selben Ordner wie das Installationsprogramm von Full Disk Encryption.

TABELLE 6-2. Vom Installationsprogramm überprüfte Bedingungen

SPEZIFIKATION	VORAUSSETZUNG	BESCHREIBUNG
Unterstütztes Betriebssystem	Nicht alle Betriebssysteme werden unterstützt	Full Disk Encryption kann nicht unter bestimmten Versionen von Windows installiert werden.

Spezifikation	Voraussetzung	Beschreibung
Die Encryption Management for Microsoft BitLocker ist bereits installiert.	Kein anderes Programm zur Festplattenverschlüsselung darf installiert sein.	Die Encryption Management for Microsoft BitLocker darf nicht installiert sein. Deinstallieren Sie die Encryption Management for Microsoft BitLocker, um Full Disk Encryption zu installieren, oder verwenden Sie stattdessen die Encryption Management for Microsoft BitLocker.
Feste Medien	Interne Festplatte	Full Disk Encryption kann nicht auf Wechseldatenträgern installiert werden, auf denen Windows ausgeführt wird.
Mehrere Festplatten	Nur eine Festplatte ist zulässig.	Auf dem Endpunkt darf sich nur eine Festplatte befinden. Umgebungen mit mehreren Festplatten werden nicht unterstützt.
Freier Speicher	Mindestens 256MB	
Arbeitsspeicher	Mindestens 512MB 1GB empfohlen	
Partitionsanzahl	Weniger als 25 Partitionen	Partitionen mit erweiterten MBRs sind nicht verfügbar.
Partitionstyp	Nur MBR wird unterstützt	GUID-Partitionstabelle (erforderlich für Festplatten, die größer als 2 TB sind) wird gegenwärtig nicht unterstützt.
Physisches Laufwerk ist bootfähig	Eine bootfähige Partition ist erforderlich.	Full Disk Encryption muss auf einer bootfähigen Partition installiert werden.

SPEZIFIKATION	VORAUSSETZUNG	BESCHREIBUNG
SCSI-Festplatte	ATA-, AHCI- oder IRRT-Festplattencontroller. SCSI wird nicht unterstützt.	• Die Prüfung gibt nur eine Warnung aus, da Windows ein SATA-Laufwerk möglicherweise als SCSI-Laufwerk meldet. • Wenn es sich bei der Festplatte nicht um echtes SCSI-Laufwerk handelt, kann Full Disk Encryption installiert werden. Wenn Sie sich nicht sicher sind, nehmen Sie eine physische Überprüfung des Laufwerks vor.
Microsoft .Net Framework	.NET 2.0 SP1 oder neuer ist erforderlich für Windows XP oder früher.	Wird für Windows Vista oder neuere Betriebssysteme weggelassen.
SED-Hardwarekompatibilität	Hardware-Verschlüsselung ist aktiviert, falls vorhanden.	Full Disk Encryption unterstützt momentan Seagate™ DriveTrust™ und OPAL-kompatible Laufwerke.
BitLocker ist aktiviert	BitLocker muss deaktiviert sein.	Full Disk Encryption und BitLocker können nicht gleichzeitig für die Festplattenverschlüsselung verantwortlich sein.



Hinweis

Wenn die Präinstallationsprüfung aus einem dieser Gründe fehlschlägt, wenden Sie sich für weitere Hilfe an Trend Micro.

Den Full Disk Encryption Agent installieren

Nach der Installation des Agent wird der Endpunkt für Software-basierte Verschlüsselung neu gestartet oder für Hardware-basierte Verschlüsselung heruntergefahren. Nach dem Neustart des Endpunkts werden die Richtlinien mit PolicyServer synchronisiert.



Hinweis

- Sie dürfen Full Disk Encryption nicht auf Endpunkte mit mehreren Festplatten installieren. Umgebungen mit mehreren Festplatten werden nicht unterstützt.
- RAID- und SCSI-Festplatten werden nicht unterstützt.
- Full Disk Encryption für Windows 8 unterstützt keine RAID-, SCSI- oder eDrive-Laufwerke.



Hinweis

Informationen zu Endpoint Encryption Diensten, die von Endpoint Encryption Agents genutzt werden, finden Sie unter *Endpoint Encryption Dienste auf Seite D-1*.

Prozedur

1. Kopieren Sie das Installationspaket auf die lokale Festplatte.
2. Starten Sie `TMFDEInstall.exe`.

   Hinweis

   Wenn das Fenster **Benutzerkontensteuerung** angezeigt wird, klicken Sie auf **Ja**, damit das Installationsprogramm Änderungen am Endpoint Encryption Gerät vornehmen kann.

3. Warten Sie, bis das Installationsprogramm geladen wurde.



ABBILDUNG 6-1. Symbol "Installation wird geladen"

Nach kurzer Zeit wird das Fenster "Willkommen" der Installation angezeigt.

4. Wählen Sie **Verwaltete Installation**, und klicken Sie anschließend auf **Weiter**.

   Das Fenster **Verwaltete Installation** wird angezeigt.

5. Die PolicyServer Informationen angeben.

OPTION	BEZEICHNUNG
Servername:	Geben Sie die IP-Adresse oder den Host-Namen von PolicyServer einschließlich der Portnummer ein, die dieser Konfiguration zugeordnet wurde.
Unternehmen	Geben Sie das Unternehmen ein. Nur ein Unternehmen wird unterstützt.
Benutzername	Geben Sie den Benutzernamen eines Kontos ein, dass über die Berechtigung verfügt, Geräte dem Unternehmen hinzuzufügen.
Kennwort	Geben Sie das Kennwort für den Benutzernamen ein.

6. Klicken Sie im Fenster **Installation abgeschlossen** auf **Schließen**.

7. Klicken Sie im Dialogfeld auf **Ja**, um den Endpunkt neu zu starten oder herunterzufahren.

   Die Installation von Full Disk Encryption ist abgeschlossen, sobald Preboot angezeigt wird. Die Verschlüsselung der Festplatte beginnt nach dem Starten von Windows.

Nächste Maßnahme

Wenn Full Disk Encryption Preboot geladen wird, muss sich der Benutzer anmelden, bevor er auf Windows zugreifen kann. Abhängig von der Richtlinienkonfiguration muss

der Benutzer möglicherweise das Kennwort nach der Anmeldung beim Endpunkt ändern.



Hinweis

Detaillierte Erläuterungen zur Konfiguration und Verwendung des Endpoint Encryption Agent finden Sie im *Endpoint Encryption Administratorhandbuch*.

Installation der Encryption Management for Microsoft BitLocker

Mit dem Encryption Management for Microsoft BitLocker Agent können Sie Endpunkte mit Trend Micro Full Disk Encryption in einer bestehenden Windows-Infrastruktur sichern.



Hinweis

Lesen Sie das folgende Thema, bevor Sie fortfahren:

- *Systemvoraussetzungen auf Seite 2-1*
- *Vor der Installation von Endpoint Encryption Agents auf Seite 6-5*
- *Voraussetzungen für verwaltete Endpunkte auf Seite 6-5*
- *Automatisierte Verteilungen auf Seite 6-29*



Hinweis

Nach der Installation ist der Endpoint Encryption Agent inaktiv, bis die Richtlinie, die das Endpoint Encryption Gerät verschlüsseln soll, aktiviert wird. Der Endpoint Encryption Agent wird erneut inaktiviert, wenn die Verschlüsselung zu einem späteren Zeitpunkt deaktiviert wird.

Die Encryption Management for Microsoft BitLocker Agent installieren

Nach der Installation des Agent wird der Endpunkt für Software-basierte Verschlüsselung neu gestartet oder für Hardware-basierte Verschlüsselung heruntergefahren.



Hinweis

Informationen zu Endpoint Encryption Diensten, die von Endpoint Encryption Agents genutzt werden, finden Sie unter *Endpoint Encryption Dienste auf Seite D-1*.

Prozedur

1. Kopieren Sie das Installationspaket auf die lokale Festplatte.
2. Starten Sie `TMFDEInstall_BL.exe`.



Hinweis

Wenn das Fenster **Benutzerkontensteuerung** angezeigt wird, klicken Sie auf **Ja**, damit das Installationsprogramm Änderungen am Endpoint Encryption Gerät vornehmen kann.

3. Warten Sie, bis das Installationsprogramm geladen wurde.



ABBILDUNG 6-2. Symbol "Installation wird geladen"

Nach kurzer Zeit wird das Fenster "Willkommen" der Installation angezeigt.

4. Die PolicyServer Informationen angeben.

OPTION	BEZEICHNUNG
Servername:	Geben Sie die IP-Adresse oder den Host-Namen von PolicyServer einschließlich der Portnummer ein, die dieser Konfiguration zugeordnet wurde.
Unternehmen	Geben Sie das Unternehmen ein. Nur ein Unternehmen wird unterstützt.

OPTION	BEZEICHNUNG
Benutzername	Geben Sie den Benutzernamen eines Kontos ein, dass über die Berechtigung verfügt, Geräte dem Unternehmen hinzuzufügen.
Kennwort	Geben Sie das Kennwort für den Benutzernamen ein.

5. Klicken Sie auf **Installieren**.

   Die Installation der Encryption Management for Microsoft BitLocker wird begonnen. Die Installation ist nach wenigen Sekunden beendet, und das Installationsprogramm wird geschlossen.

6. Wechseln Sie in die Task-Leiste, und klicken Sie auf das -Symbol, um den Agent der Encryption Management for Microsoft BitLocker zu öffnen.



Hinweis

Detaillierte Erläuterungen zur Konfiguration und Verwendung des Endpoint Encryption Agent finden Sie im *Endpoint Encryption Administratorhandbuch*.

Installation der Encryption Management for Apple FileVault

Mit der Encryption Management for Apple FileVault Agent können Sie Endpunkte mit Trend Micro Full Disk Encryption in einer bestehenden Mac OS-Infrastruktur sichern.



Hinweis

Lesen Sie das folgende Thema, bevor Sie fortfahren:

- *Systemvoraussetzungen auf Seite 2-1*
- *Vor der Installation von Endpoint Encryption Agents auf Seite 6-5*
- *Voraussetzungen für verwaltete Endpunkte auf Seite 6-5*
- *Automatisierte Verteilungen auf Seite 6-29*

Den Agent der Encryption Management for Apple FileVault installieren

Die Encryption Management for Apple FileVault kann vom PolicyServer Gruppenadministrator, Authentifizierer oder von herkömmlichen Benutzerkonten installiert werden.



Hinweis

Informationen zu Endpoint Encryption Diensten, die von Endpoint Encryption Agents genutzt werden, finden Sie unter *Endpoint Encryption Dienste auf Seite D-1*.

Prozedur

1. Starten Sie `TMFDEInstall_FV.exe`.

   Das Datenträger-Image von Trend Micro Full Disk Encryption wird angezeigt.

2. Doppelklicken Sie auf `Trend Micro Full Disk Encryption.pkg`, um die Installation zu starten.

   Der Setup-Assistent der Encryption Management for Apple FileVault wird gestartet und beginnt mit der Installation von File Encryption.

3. Klicken Sie im Fenster **Willkommen** auf **Weiter**.

   Das Installationsprogramm überprüft, ob die Systemvoraussetzungen erfüllt werden.

4. Wenn die Systemvoraussetzungen erfüllt werden, klicken Sie auf **Installieren**.

5. Wählen Sie die Festplatte, auf der der Agent installiert werden soll.

6. Geben Sie den Benutzernamen und das Kennwort eines Kontos ein, das berechtigt ist, Anwendungen auf dem Endpunkt zu installieren, und klicken Sie auf **Agent installieren**

   Die Installation beginnt.

7. Die PolicyServer Informationen angeben.

Option	Bezeichnung
Servername:	Geben Sie die IP-Adresse oder den Host-Namen von PolicyServer einschließlich der Portnummer ein, die dieser Konfiguration zugeordnet wurde.
Unternehmen	Geben Sie das Unternehmen ein. Nur ein Unternehmen wird unterstützt.
Benutzername	Geben Sie den Benutzernamen eines Kontos ein, dass über die Berechtigung verfügt, Geräte dem Unternehmen hinzuzufügen.
Kennwort	Geben Sie das Kennwort für den Benutzernamen ein.

8. Klicken Sie auf **Fortfahren**.

   Die Installation der Encryption Management for Apple FileVault beginnt nach einigen Sekunden.

9. Klicken Sie im Anschluss an die Installation auf **Schließen**, um den Endpunkt neu zu starten.

   Der Agent der Encryption Management for Apple FileVault wird nach dem Neustart des Endpunkts sofort geladen.

10. Navigieren Sie zur Menüleiste ( ), um den Agent der Encryption Management for Apple FileVault zu öffnen.



Hinweis

Detaillierte Erläuterungen zur Konfiguration und Verwendung des Endpoint Encryption Agent finden Sie im *Endpoint Encryption Administratorhandbuch*.

Mobiles Konto für Active Directory unter Mac OS erstellen

Lokale Mac OS-Konten oder mobile Konten können die Verschlüsselung unter Mac OS X Mountain Lion oder höher einleiten. Andere Mac OS-Benutzerkontentypen sind nicht in der Lage, die Verschlüsselung einzuleiten.

Wenn ein anderes Mac OS-Konto als ein lokales oder mobiles Konto versucht, eine Verschlüsselung einzuleiten, wird die folgende Meldung angezeigt:



Die folgende Aufgabe zeigt, wie Sie ein mobiles Konto für Ihr Mac OS-Konto erstellen, um dieses Problem zu umgehen.

Prozedur

1. Navigieren Sie im Apple-Menü zu **Systemeinstellungen...**.

   Das Fenster **Systemeinstellungen** wird angezeigt.

2. Wählen Sie **Benutzergruppen** im Abschnitt **System**.

3. Klicken Sie in der unteren linken Ecke auf das Sperrsymbol.

4. Klicken Sie auf **Erstellen...** neben **Mobiles Konto**.

5. Wählen Sie in den folgenden Fenster die persönlichen Einstellungen, und klicken Sie auf **Erstellen**, um zum jeweils nächsten Fenster zu gelangen.

6. Wenn Sie dazu aufgefordert werden, geben Sie Ihr Active Directory-Kennwort ein, und klicken Sie auf **OK**.



Ihr mobiles Konto wurde erstellt. Sie können nun mit diesem mobilen Konto die Verschlüsselung einleiten.

File Encryption Verteilung

In diesem Abschnitt wird die Installation des File Encryption Agent beschrieben. Mit File Encryption können Sie die Dateien und Ordner auf nahezu jedem Gerät, das als Laufwerk im Host-Betriebssystem angezeigt wird, schützen.



Hinweis

Es ist nun möglich, mit den Rollen des Unternehmensadministrators und Unternehmensauthentifizierers die Endpoint Encryption Agents zu installieren.

Übersicht über die Verteilung mit File Encryption

Prozedur

1. Aktivieren Sie File Encryption in PolicyServer MMC.
2. Konfigurieren Sie die Richtlinien für File Encryption:

a. Verwendeter Verschlüsselungsschlüssel

b. Zu verschlüsselnde Ordner

c. Verwendung von Wechselmedien

d. Authentifizierungsmethode

3. Richten Sie Benutzer und Gruppen ein.

4. Erstellen und testen Sie das Installationspaket in einem Pilotprogramm.

Siehe *Pilotverteilung von Endpoint Encryption auf Seite C-1*.

5. Überprüfen Sie, ob die festgelegten Richtlinieneinstellungen erzwungen werden.

a. Legen Sie den verschlüsselten Ordner fest.

Weitere Informationen finden Sie unter *Verschlüsselte Ordner von File Encryption auf Seite 6-25*.

b. Legen Sie den Verschlüsselungsschlüssel fest.

Weitere Informationen finden Sie unter *File Encryption Verschlüsselungsschlüssel auf Seite 6-26*.

c. Legen Sie die Richtlinien für das Speichergerät fest.

Weitere Informationen finden Sie unter *Schutz für Speichergeräte mit File Encryption auf Seite 6-27*.

6. Bereiten Sie die Endbenutzer-Kommunikation vor.

Weitere Informationen finden Sie unter *Endbenutzer-Kommunikation auf Seite B-12*.

Verschlüsselte Ordner von File Encryption

File Encryption kann mit dem installierten File Encryption Agent auf den Endpunkten automatisch verschlüsselte Ordner anlegen. Dateien, die in einen geschützten Ordner kopiert werden, werden automatisch verschlüsselt. In der Standardeinstellung wird ein von File Encryption verschlüsselter Ordner auf dem Desktop erstellt.

In der folgenden Tabelle werden die Voraussetzungen an die Richtlinien erklärt, um den verschlüsselten Ordner von File Encryption zu konfigurieren. Abhängig von der

verwendeten Management-Konsole gibt es leichte Abweichungen bei der Richtlinienkonfiguration.

TABELLE 6-3. Richtlinienkonfiguration für verschlüsselte Ordner

KONSOLE	RICHTLINIENEINSTELLUNG
Control Manager	Greifen Sie auf eine neue oder vorhandene Richtlinie zu (**Richtlinien** > **Richtlinienverwaltung**), und erweitern Sie **File Encryption**. Erstellen Sie mit **Zu verschlüsselnde Ordner** auf dem Endpunkt sichere Ordner.
PolicyServer MMC	• Erstellen Sie mit **File Encryption** > **Verschlüsselung** > **Ordner zum Verschlüsseln angeben** sichere Ordner auf dem Endpunkt. • Erstellen Se mit **File Encryption** > **Verschlüsselung** > **Wechselmedien** > **Zu verschlüsselnde Ordner auf Wechselmedien** sichere Ordner auf einem USB-Speichergerät.

File Encryption Verschlüsselungsschlüssel

Mit dem File Encryption Verschlüsselungsschlüssel legen Sie die Zugriffstufe für den Zugriff auf verschlüsselte Ordner von File Encryption fest.

- **Benutzerschlüssel**: Nur der Benutzer kann auf den verschlüsselten Inhalt zugreifen.
- **Gruppenschlüssel**: Nur Benutzer innerhalb derselben Richtlinie (Control Manager) oder derselben Gruppe (PolicyServer MMC) können auf den Inhalt zugreifen.
- **Unternehmensschlüssel**: Alle Benutzer von Endpoint Encryption können auf den Inhalt zugreifen.

TABELLE 6-4. Richtlinienkonfiguration für den Verschlüsselungsschlüssel

KONSOLE	RICHTLINIENEINSTELLUNG
Control Manager	Greifen Sie auf eine neue oder vorhandene Richtlinie zu (**Richtlinien** > **Richtlinienverwaltung**), und erweitern Sie **File Encryption**. Legen Sie den Schlüssel mit **Verwendeter Verschlüsselungsschlüssel** fest.
PolicyServer MMC	• Legen Sie mit **File Encryption** > **Verschlüsselung** > **Zulässige Verschlüsselungsmethode** fest, welche Schlüssel verfügbar sind • Legen Sie mit **File Encryption** > **Verschlüsselung** > **Verwendeter Verschlüsselungsschlüssel** den Schlüssel fest

Schutz für Speichergeräte mit File Encryption

Mit File Encryption können Dateien auf Wechselmedien geschützt werden. Folgende Optionen sind verfügbar:

- **Wechselmedien**: Aktiviert den Schutz für USB-Speichergeräte.
- **Zulässige USB-Geräte**: Sie können alle USB-Speichergeräte oder nur KeyArmor Geräte zulassen.
- **Gerät vollständig verschlüsseln**: FileAmor verschlüsselt automatisch alle Dateien, die auf das USB-Speichergerät kopiert werden.
- **USB-Laufwerk deaktivieren**: Geben Sie an, ob das USB-Laufwerk immer, nie oder nur, wenn nicht angemeldet, deaktiviert werden soll.

TABELLE 6-5. Richtlinienkonfigurationen für Speichergeräte

KONSOLE	RICHTLINIENEINSTELLUNG
Control Manager	Greifen Sie auf eine neue oder vorhandene Richtlinie zu (**Richtlinien** > **Richtlinienverwaltung**), und erweitern Sie **File Encryption**. Legen Sie die Richtlinien im Abschnitt **Speichergeräte** fest.
PolicyServer MMC	Navigieren Sie zu **File Encryption** > **Verschlüsselung**.

File Encryption Installation

Mit File Encryption können Sie die Dateien und Ordner auf nahezu jedem Gerät, das als Laufwerk im Host-Betriebssystem angezeigt wird, schützen.



Hinweis

Lesen Sie das folgende Thema, bevor Sie fortfahren:

- *Systemvoraussetzungen auf Seite 2-1*
- *Vor der Installation von Endpoint Encryption Agents auf Seite 6-5*
- *Voraussetzungen für verwaltete Endpunkte auf Seite 6-5*
- *Automatisierte Verteilungen auf Seite 6-29*

Den File Encryption Agent installieren

Der File Encryption Installationsvorgang besteht aus dem Ausführen eines Installationsprogramms auf dem Endpunkt und dem Durchführen der schrittweisen Anweisungen.



Hinweis

Informationen zu Endpoint Encryption Diensten, die von Endpoint Encryption Agents genutzt werden, finden Sie unter *Endpoint Encryption Dienste auf Seite D-1*.

Prozedur

1. Führen Sie `FileEncryptionIns.exe` aus.

   Der Assistent zur Einrichtung von File Encryption wird angezeigt.

2. Klicken Sie auf **Weiter**.

   Hinweis

   Wenn Sie eine Nachfrage von der Benutzerkontensteuerung erhalten, klicken Sie auf **Ja**.

Das Installationsprogramm von File Encryption wird gestartet, und der Agent wird automatisch installiert.

3. Warten Sie, bis der File Encryption Agent installiert wird.
4. Wenn die Installation abgeschlossen ist, klicken Sie auf **Schließen**.
5. Klicken Sie auf **Ja**, um Windows neu zu starten.

   Der Endpunkt wird neu gestartet, und File Encryption wird installiert. Es werden zwei Symbole für File Encryption angezeigt: eine Verknüpfung auf dem Desktop und ein Symbol in der Task-Leiste. Nach dem Laden des Desktops dauert es möglicherweise einen Moment, bis der Agent initialisiert wird.

6. Legen Sie im Fenster **Anmelden** von File Encryption die folgenden Parameter fest.

OPTION	BEZEICHNUNG
Benutzername	Geben Sie den Benutzernamen eines Kontos ein, dass über die Berechtigung verfügt, Geräte dem Unternehmen hinzuzufügen.
Kennwort	Geben Sie das Kennwort für den Benutzernamen ein.
Servername:	Geben Sie die IP-Adresse oder den Host-Namen von PolicyServer einschließlich der Portnummer ein, die dieser Konfiguration zugeordnet wurde.
Unternehmen	Geben Sie das Unternehmen ein. Nur ein Unternehmen wird unterstützt.

7. Klicken Sie auf **OK**.



Hinweis

Detaillierte Erläuterungen zur Konfiguration und Verwendung des Endpoint Encryption Agent finden Sie im *Endpoint Encryption Administratorhandbuch*.

Automatisierte Verteilungen

Die skriptgesteuerte Installationsmethode wird bei großen Verteilungen mit Hilfe von automatischen Tools wie Microsoft SMS oder Active Directory am häufigsten

verwendet. Command Line Installer Helper (weitere Details unter *Command Line Installer Helper auf Seite 6-32*) ist ein Tool zum Erstellen von Skripts. Die verfügbaren Argumente unterstützen vollständig oder teilweise unbeaufsichtigte Installationen.



Warnung!

Eine unzureichende Einrichtung des Systems oder Vorbereitung der Festplatte kann zu irreversiblen Datenverlusten führen.

Verteilung von Endpoint Encryption Agent mit OfficeScan

In Umgebungen, in denen OfficeScan verwendet wird, ist das Plug-in "Endpoint Encryption Verteilungstool" die effizienteste Verteilungsmethode. Informationen zur Verwendung des Plug-in finden Sie unter *Integration von OfficeScan auf Seite 7-1*.

Voraussetzungen für Verteilungen unter Verwendung von Skripts

- Sie können Skripts mit dem Command Line Helper oder Command Line Helper Installationsprogramm definieren.
- Rufen Sie das Skript vom Endpunkt aus auf und nicht von einer Netzwerkfreigabe oder einem USB-Laufwerk.
- Systemverwaltungs-Software: Tivoli, SCCM/SMS oder LANDesk
- Der Benutzer, der die Installationsskripts aufruft, muss über ein lokales Administratorkonto verfügen.
- Empfehlung: Sie sollten Installationsskripts in einem Pilotprogramm testen, bevor Sie eine Massenverteilung durchführen. Empfehlungen zum Pilotprogramm finden Sie unter *Pilotverteilung von Endpoint Encryption auf Seite C-1*.

Skriptargumente

In der nachfolgenden Tabelle werden die Argumente zum Aufbau von Skripts zur automatischen Installation von Agents erläutert.

TABELLE 6-6. Full Disk Encryption Skriptargumente

ARGUMENT	WERT	HINWEISE
ENTERPRISE	Der Name des Unternehmens	Der Name des Unternehmens.
HOST	DNS-Host-Name oder IP-Adresse	Der Name oder Standort von PolicyServer.
USERNAME	• Gruppenadministrator • Gruppenauthentifizierer • Gruppenbenutzer (wenn die Richtlinie zum Erlauben der Installation aktiviert ist)	Ein Unternehmensadministrator- oder -authentifiziererkonto kann nicht zur Installation von Full Disk Encryption verwendet werden.
PASSWORD	Kennwort für den angegebenen Benutzernamen	Das feste Kennwort, das in PolicyServer für den Benutzer konfiguriert wurde, oder ein Domänenkennwort.



Hinweis

Die Encryption Management for Microsoft BitLocker verwendet dasselbe Skript wie Full Disk Encryption.

TABELLE 6-7. Argumente für File Encryption-Skripts

ARGUMENT	WERT	HINWEISE
PSENTERPRISE	Der Name des Unternehmens	Der Name des Unternehmens.
PSHOST	DNS-Host-Name oder IP-Adresse	Der Name oder Standort von PolicyServer.
FAUSERNAME	• Gruppenadministrator • Gruppenauthentifizierer • Gruppenbenutzer (wenn die Richtlinie zum Erlauben der Installation aktiviert ist)	Ein Unternehmensadministrator- oder -authentifiziererkonto kann nicht zur Installation von File Encryption verwendet werden.

Argument	Wert	Hinweise
FAPASSWORD	Kennwort für den angegebenen Benutzernamen	Das feste Kennwort, das in PolicyServer für den Benutzer konfiguriert wurde, oder ein Domänenkennwort.

Command Line Installer Helper

Full Disk Encryption und File Encryption sind mit Tools zur automatischen Software-Verteilung kompatibel, beispielsweise mit SMS, SCCM, Tivoli, GPO und LANDesk. Mit Command Line Installer Helper können Sie Skripts generieren, um beliebige Trend Micro Endpoint Encryption Produkte zu installieren. Über die Optionen können die Installationskontodaten verschlüsselt und verborgen sowie verschiedene Optionen für die Eingabe ausgewählt werden. Skriptergebnisse können zum Exportieren auf einfache Weise in die Zwischenablage kopiert werden.



Hinweis

Die Befehlszeileninstallation von PolicyServer wird von den Versionen 3.1.2 und höher unterstützt.

Beim Verwenden von Command Line Installer Helper:

- Führen Sie Installationsskripts nur auf einem Endpunkt aus, nicht über das Netzwerk.
- Der Benutzer, der die Skripts aufruft, muss über ein lokales Administratorkonto verfügen.
- Sie sollten Installationsskripts in einem Pilotprogramm testen, bevor Sie eine Massenverteilung durchführen.
- Überprüfen Sie, ob alle Installationsvoraussetzungen von Full Disk Encryption und File Encryption erfüllt sind, bevor Sie eine Massenverteilung der Software durchführen.

Agent-Installationsskripts erstellen

Die folgenden Informationen sind erforderlich, um ein Skript für die unbeaufsichtigte Installation zu generieren: Host-Name oder IP-Adresse des PolicyServer, Name des Unternehmens, Benutzername, Kennwort sowie Pfad und Versionsnummer des Endpunkt-Client-Installationsprogramms. Sie finden den Command Line Installer Helper im Installationsverzeichnis im Ordner **Tools**.

Prozedur

1. Doppelklicken Sie auf `CommandLineInstallerHelper.exe`.

   Das Fenster **Command Builder** wird angezeigt.

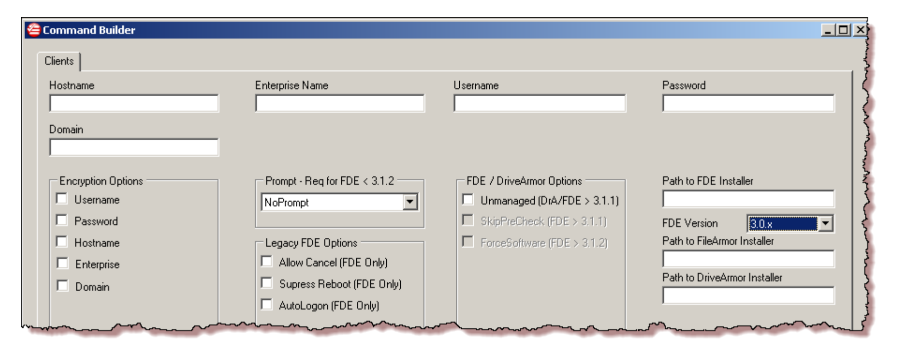


ABBILDUNG 6-3. Command Line Helper Installationsprogramm

2. Geben Sie den Servernamen des erforderlichen PolicyServer (Host-Name), das Unternehmen und den Benutzernamen und das Kennwort des Unternehmensadministrators ein.

OPTION	BEZEICHNUNG
Servername:	Geben Sie die IP-Adresse oder den Host-Namen von PolicyServer einschließlich der Portnummer ein, die dieser Konfiguration zugeordnet wurde.
Unternehmen	Geben Sie das Unternehmen ein. Nur ein Unternehmen wird unterstützt.

OPTION	BEZEICHNUNG
Benutzername	Geben Sie den Benutzernamen eines Kontos ein, dass über die Berechtigung verfügt, Geräte dem Unternehmen hinzuzufügen.
Kennwort	Geben Sie das Kennwort für den Benutzernamen ein.

3. Wählen Sie die Verschlüsselungsoptionen aus.
   - Benutzername
   - Kennwort
   - Host-Name
   - Unternehmen
   - Domäne
4. Wählen Sie, ob Eingabeaufforderungen für den Endbenutzer angezeigt oder eine unbeaufsichtigte Installation durchgeführt werden soll.
5. Geben Sie ältere Optionen an, die nur ältere Versionen von Full Disk Encryption Agent betreffen.
   - **Allow Cancel**: Der Endbenutzer darf die Installation abbrechen.
   - **Suppress Reboot**: Der Endpunkt wird nach der Installation nicht neu gestartet.
   - **Autologon**: Nach der Installation des Full Disk Encryption Agent wird der Benutzer automatisch bei Full Disk Encryption Preboot angemeldet, und der Endpunkt wird neu startet.
6. Geben Sie den Pfad zu den Installationsdateien an.
7. Klicken Sie auf **Generate Command**.

   Das Skript wird generiert.
8. Klicken Sie auf die entsprechende Schaltfläche, um den Befehl zu kopieren.

   Das resultierende Skript wird in die Zwischenablage kopiert.

9. Fügen Sie den Befehl in das Installationsskript ein.

Command Line Helper

Mit Command Line Helper können verschlüsselte Werte erzeugt werden, die als sichere Anmeldedaten beim Erstellen von Installationsskripts oder für DAAutoLogin verwendet werden können. Command Line Helper befindet sich im Ordner `Tools`.



Hinweis

Der Command Line Helper kann nur auf Systemen ausgeführt werden, auf denen Trend Micro Endpoint Encryption Produkte installiert sind, da die Kryptographie von Mobile Armor genutzt wird.

Der Command Line Helper akzeptiert eine einzelne Zeichenfolge als Argument und gibt einen verschlüsselten Wert zurück, der im Installationsskript verwendet werden kann. Die vorangestellten und nachgestellten “=”-Zeichen sind Teil der gesamten verschlüsselten Zeichenfolge und müssen auf der Befehlszeile angegeben werden. Wenn der verschlüsselte Wert kein vorangestelltes "="-Zeichen enthält, müssen Sie es in das Skript einfügen.

Über die Optionen können die Installationskontodaten verschlüsselt und verborgen sowie verschiedene Optionen für die Eingabe ausgewählt werden. Skriptergebnisse können zum Exportieren auf einfache Weise in die Zwischenablage kopiert werden.

Tabelle 6-8. Argumente für Command Line Helper

Funktion	Argumente		
	Full Disk Encryption	Full Disk Encryption verschlüsselt	File Encryption
Unternehmen	**ENTERPRISE**	**eENTERPRISE**	
PolicyServer	**HOST**	**eHOST**	**PSHOST**
Benutzername	**USERNAME**	**eUSERNAME**	**FAUSERNAME**

FUNKTION	ARGUMENTE		
	FULL DISK ENCRYPTION	FULL DISK ENCRYPTION VERSCHLÜSSELT	FILE ENCRYPTION
Kennwort	**PASSWORD**	**ePASSWORD**	**FAPASSWORD**



Hinweis

Das Installationsprogramm von File Encryption bearbeitet automatisch verschlüsselte Werte.

Full Disk Encryption Skriptbeispiel

Nur ein Wert kann an Command Line Helper übergeben werden. Dieser kann jedoch so oft wie nötig ausgeführt werden, um alle erforderlichen verschlüsselten Werte zu sammeln.

`Speicherort der Software = C:\Programme\Trend Micro\Full Disk Encryption\TMFDEInstaller.exe`

`ENTERPRISE = MyCompany`

`HOST = PolicyServer.mycompany.com`

`eUSERNAME = GroupAdministrator`

`ePASSWORD = 123456`



Hinweis

In diesem Beispiel werden der Benutzername und das Kennwort verschlüsselt.

Ausgabe zum Installieren von Full Disk Encryption:

```
C:\Program Files\Trend Micro\
Full Disk Encryption\TMFDEInstaller.exe
ENTERPRISE=MyCompany HOST= PolicyServer.mycompany.com
```

```
eUSERNAME==jJUJC/Lu4C/Uj7yYwxubYhAuCrY4f7AbVFp5hKo2PR4O
ePASSWORD==5mih67uKdy7T1VaN2ISWGQQ=
```

Beispiel für File Encryption-Skripts

Dabei handelt es sich um ein Beispiel für ein Installationsskript zur Installation von File Encryption.

```
Software location = C:\Program Files\Trend Micro\File
Encryption\FileEncryptionIns.exe

PSEnterprise = MyCompany

PSHost = PolicyServer.mycompany.com

FAUser = GroupAdministrator

FAPassword = 123456
```



Hinweis

In diesem Beispiel werden der Benutzername und das Kennwort verschlüsselt.

Ausgabe zur Installation von File Encryption:

```
C:\Program Files\Trend Micro\
File Encryption\FileEncryptionIns.exe
PSEnterprise=MyCompany PSHost= PolicyServer.mycompany.com
FAUser==jJUJC/Lu4C/Uj7yYwxubYhAuCrY4f7AbVFp5hKo2PR4O=
FAPassword==5mih67uKdy7T1VaN2ISWGQQ=
```

Command Line Helper

Administratoren können mit Command Line Helper zusammen mit DAAutoLogin eine problemlose Patch-Verwaltung mit Full Disk Encryption durchführen. Mit Command Line Helper können Sie über ein Installationsskript verschlüsselte Werte an Full Disk Encryption Preboot übergeben. `DAAutoLogin` lässt das einmalige Umgehen von Full Disk Encryption Preboot zu.

Prozedur

1. Kopieren Sie `CommandLineHelper.exe` auf die lokale Festplatte des Computers, auf dem Full Disk Encryption installiert ist.

   Beispiel: Kopieren Sie `CommandLineHelper.exe` auf das Laufwerk `C:\`.

2. Öffnen Sie ein Eingabeaufforderungsfenster, geben Sie `C:\CommandLineHelper.exe` ein, und geben Sie anschließend den Benutzernamen oder das Kennwort ein.

   Wenn der Benutzername beispielsweise "SMSUser" ist, geben Sie folgenden Befehl ein:

   ```
   C:\CommandLineHelper.exe SMSUser
   ```

3. Drücken Sie die EINGABETASTE, um den verschlüsselten Wert anzuzeigen.

4. Führen Sie Command Line Helper erneut aus, um den zweiten Wert zu verschlüsseln. Falls Sie zunächst den Benutzernamen verschlüsselt haben, verschlüsseln Sie im zweiten Durchgang das Kennwort.

Upgrade

Um Zugriff auf neue Produktfunktionen zu erhalten oder eine ältere Agent-Software zu aktualisieren, um die Endpunktsicherheit zu verbessern, müssen Administratoren möglicherweise den Endpoint Encryption PolicyServer und alle verwalteten Endpunkte aktualisieren, auf denen ein Endpoint Encryption Agent ausgeführt wird. Um die Synchronisierung der Richtlinien und die Sicherheit der Informationen zu gewährleisten, müssen Sie PolicyServer immer vor den Endpoint Encryption Agents aktualisieren.

In diesem Abschnitt wird beschrieben, wie auf sichere Weise ein Upgrade von Endpoint Encryption, einschließlich PolicyServer, PolicyServer MMC und der Software für den Endpoint Encryption Agent, auf die neuesten Versionen durchgeführt werden kann.



Warnung!

Stellen Sie vor der Aktualisierung des Agent sicher, dass PolicyServer zuerst auf Version 5.0 Patch 1 aktualisiert wird. Endpoint Encryption 5.0 Patch 1 Agents können nicht mit PolicyServer 3.1.3 oder früher kommunizieren.

Den Endpunkt auf Windows 8 aktualisieren

Endpoint Encryption unterstützt kein Upgrade auf Windows 8. Ist ein Upgrade erforderlich, empfiehlt Trend Micro folgende Vorgehensweise, um einen Datenverlust zu vermeiden, wenn Full Disk Encryption oder File Encryption bereits auf dem Agent installiert ist.

Prozedur

1. Entschlüsseln Sie den Endpunkt.

   Weitere Informationen finden Sie im entsprechenden Abschnitt für den Agent im *Endpoint Encryption Administratorhandbuch*.

2. Deinstallieren Sie den Agent.

   - Informationen zur Verwendung von OfficeScan finden Sie unter *Mit OfficeScan Endpoint Encryption Agents deinstallieren auf Seite 6-58*.
   - Informationen zur Deinstallation von Full Disk Encryption finden Sie unter *Full Disk Encryption deinstallieren auf Seite 6-53*.
   - Informationen zur Deinstallation von File Encryption finden Sie unter *File Encryption deinstallieren auf Seite 6-56*.
   - Informationen zur manuelle Deinstallation der Encryption Management for Microsoft BitLocker finden Sie unter *Encryption Management for Microsoft BitLocker deinstallieren auf Seite 6-55*.

3. Installieren Sie das Betriebssystem Windows 8.



Hinweis

In dieser Dokumentation wird die Installation von Windows 8 nicht beschrieben. Anweisungen finden Sie in der entsprechenden Dokumentation von Microsoft.

4. Stellen Sie sicher, dass die Windows 8-Umgebung stabil ist und dass das Upgrade erfolgreich durchgeführt wurde.

5. Installieren Sie die Agent-Anwendungen erneut:

    - Informationen über das Installieren von Full Disk Encryption finden Sie unter *Full Disk Encryption Verteilung auf Seite 6-6*.

    - Informationen über das Installieren von File Encryption finden Sie unter *File Encryption Verteilung auf Seite 6-24*.

Upgrade von Full Disk Encryption

Vorbereitungen

- Verifizieren Sie *Full Disk Encryption Systemvoraussetzungen auf Seite 2-10*

- Lesen Sie *Upgrade-Pfade auf Seite 3-24*.

Aktualisieren Sie mit dem Installationsprogramm von Full Disk Encryption den Agent von Full Disk Encryption 3.1.3 SP1 auf Full Disk Encryption 5.0 Patch 1. Informationen zu früheren Versionen von Full Disk Encryption finden Sie in der begleitenden Dokumentation, die Sie unter folgender Adresse herunterladen können:

http://docs.trendmicro.com/de-de/enterprise/endpoint-encryption.aspx

---

Prozedur

1. Kopieren Sie das Installationspaket auf die lokale Festplatte.

2. Starten Sie `TMFDEInstall.exe`.



Hinweis

Wenn das Fenster **Benutzerkontensteuerung** angezeigt wird, klicken Sie auf **Ja**, damit das Installationsprogramm Änderungen am Endpoint Encryption Gerät vornehmen kann.

Die folgende Nachricht wird über der Task-Leiste angezeigt.



3. Warten Sie, bis die Aktualisierung abgeschlossen wurde.

4. Klicken Sie im Bestätigungsdialogfeld auf **Ja**, um den Endpunkt neu zu starten.

Wichtige Hinweise für MobileArmor Full Disk Encryption Service Pack 7 und niedriger

Bei einer Aktualisierung des als MobileArmor bezeichneten Full Disk Encryption Agent Service Pack 6 und niedriger:

- Überprüfen Sie im BIOS, ob der Festplatten-Controller auf ATA- oder AHCI-Modus eingestellt ist.
- Bei Laptops mit einem Multi-Bay-Gehäuse dürfen Sie den Agent nur installieren, wenn das Laptop nicht angedockt ist.

Intel™Rapid Recovery Technology (IRRT):

- Einige neuere Systeme unterstützen IRRT im BIOS.
- Wenn für den BIOS-Festplattencontroller der IRRT-Modus festgelegt ist, müssen Sie diesen vor der Installation von Full Disk Encryption in den AHCI-Modus ändern.
- IRRT muss vom Betriebssystem unterstützt werden.

Intel™ Matrix Manager-Software:

- Standardmäßig ist unter Window XP die Intel Matrix Manager-Software nicht installiert. Die Einstellungen müssen im BIOS ohne eine erneute Neuinstallation des Betriebssystems vorgenommen werden.

- Unter Windows Vista ist die Intel Matrix Manager-Software standardmäßig installiert.



Hinweis

Wenn die Einstellung für den SATA-Betrieb unter Windows Vista geändert und Full Disk Encryption installiert wird, wird Windows nicht gestartet. Ändern Sie die Einstellung wieder in IRRT, und Vista wird normal geladen.

File Encryption aktualisieren

Vorbereitungen

- Verifizieren Sie *Systemvoraussetzungen für File Encryption auf Seite 2-14*
- Lesen Sie *Upgrade-Pfade auf Seite 3-24*.

Mit `FileEncryptionIns.exe` können Sie den Agent von einer früheren Version aktualisieren.



Hinweis

`FileEncryptionIns.exe` umgeht die Einstellung "Deinstallation durch Benutzer zulassen" und führt die Aktualisierung durch, unabhängig davon, ob für die Richtlinie **Ja** oder **Nein** festgelegt wurde.

Prozedur

1. Führen Sie `FileEncryptionIns.exe` aus.

   Windows Installer deinstalliert den älteren File Encryption Agent (FileArmor), und installiert anschließend File Encryption 5.0 Patch 1.

2. Warten Sie, bis der Endpunkt neu gestartet wurde.

3. Melden Sie sich nach dem Neustart von Windows an, und prüfen Sie den neuen File Encryption Ordner. Verschlüsselte Dateien und Ordner werden beibehalten.

Encryption Management for Apple FileVault aktualisieren

Das Upgrade entspricht im Wesentlichen der Installation. Sorgen Sie dafür, dass Sie die Daten für PolicyServer griffbereit haben.

Prozedur

- Führen Sie *Den Agent der Encryption Management for Apple FileVault installieren auf Seite 6-21* durch.

Encryption Management for Microsoft BitLocker aktualisieren

Prozedur

1. Führen Sie *Encryption Management for Microsoft BitLocker deinstallieren auf Seite 6-55* durch.
2. Warten Sie, bis die Entschlüsselung abgeschlossen ist. Der Benutzer kann den Endpunkt ganz normal verwenden.
3. Installieren Sie die Encryption Management for Microsoft BitLocker, wie unter *Die Encryption Management for Microsoft BitLocker Agent installieren auf Seite 6-18* beschrieben.

Migration

Administratore müssen möglicherweise Endpoint Encryption Geräte migrieren, wenn Mitarbeiter in eine andere Abteilung oder an einen anderen Standort versetzt werden. Eine PolicyServer Instanz kann mehrere Unternehmenskonfigurationen haben, die einen Geschäftsbereich oder eine Abteilung repräsentieren.

Wenn Sie ein Gerät in ein neues Unternehmen verschieben, wird das Endpoint Encryption Gerät aus dem alten Unternehmen entfernt und dem neuen Unternehmen innerhalb derselben PolicyServer Instanz hinzugefügt.

Wenn Sie ein Endpoint Encryption Gerät zu einem neuen PolicyServer verschieben, wird das Endpoint Encryption Gerät nicht vom alten PolicyServer entfernt, sondern die Netzwerkkonfiguration im Endpoint Encryption Agent wird so geändert, dass der Agent auf die neue PolicyServer Instanz verweist.

Installiertes Verschlüsselungsprodukt ersetzen

Sie können Full Disk Encryption auf einem Gerät installieren, das vorher mit einer anderen Software zur Full Disk Encryption verschlüsselt wurde. Da die meisten Full Disk Encryption-Programme jeden Sektor der Festplatte ändern, ist es sehr wichtig, dass Sie das Verfahren zur Vorbereitung der Festplatte und die Verteilungsmethode testen. Je nachdem, wie lange es dauert, ein Gerät zu entschlüsseln und mit Full Disk Encryption zu verschlüsseln, ist es ggf. sinnvoll, vor der Installation von Full Disk Encryption einfach die Benutzerdaten zu sichern und ein neues Image des Endpunkts aufzuspielen.

Möglichkeit 1: Installiertes Verschlüsselungsprodukt entfernen

Prozedur

1. Entschlüsseln Sie die Festplatte gemäß der vom Softwareanbieter angegebenen Methode.
2. Deinstallieren Sie die Software des Anbieters (oder stellen Sie sicher, dass die BitLocker-Verschlüsselung deaktiviert ist).
3. Starten Sie das Gerät neu.
4. Führen Sie den Befehl `chkdsk` aus und defragmentieren Sie das Laufwerk.
5. Überprüfen Sie auf jedem Gerät, ob ein normaler Master Boot Record (MBR) vorliegt, und vergewissern Sie sich, dass ein normaler Bootsektor auf der Bootpartition vorhanden ist.



Hinweis

Das Gerät darf nicht über zwei bootfähige Betriebssysteme verfügen.

6. Sichern Sie die Benutzerdateien.

7. Installieren Sie Full Disk Encryption. Weitere Informationen finden Sie unter *Full Disk Encryption Installation auf Seite 6-12*.

Möglichkeit 2: Sicherung durchführen und neues Image auf den Endpunkt aufspielen

Prozedur

1. Sichern Sie die Benutzerdateien.

2. Spielen Sie ein Image des Laufwerks auf:

   a. Führen Sie über eine Befehlszeile `DiskPart Clean All` aus.

   b. Erstellen Sie eine Partition.

   c. Formatieren Sie das Laufwerk.

   d. Spielen Sie ein Image des Laufwerks auf.

3. Installieren Sie Full Disk Encryption, und verschlüsseln Sie den Endpunkt.

4. Stellen Sie die Benutzerdateien wieder her.

PolicyServer Einstellungen für Full Disk Encryption

Sie können die PolicyServer Einstellungen für Full Disk Encryption konfigurieren, indem Sie von Full Disk Encryption Preboot aus die Wiederherstellungskonsole öffnen oder indem Sie die Datei `C:\Program Files\Trend Micro\Full Disk Encryption\RecoveryConsole.exe` ausführen.

Voraussetzung für die Wiederherstellungskonsole

Mit der Full Disk Encryption Wiederherstellungskonsole können Sie die PolicyServer Einstellungen ändern.

Von Full Disk Encryption Preboot auf die Wiederherstellungskonsole zugreifen

Nur Unternehmens- oder Gruppenadministrator- und -authentifiziererkonten können auf die Wiederherstellungskonsole zugreifen.

Prozedur

1. Aktivieren Sie die folgende Richtlinie, um Benutzern zu erlauben, auf die Wiederherstellungskonsole zuzugreifen:

   Full Disk Encryption > **Agent** > **Wiederherstellung durch Benutzer zulassen**

2. Starten Sie den Endpunkt neu.

   Full Disk Encryption Preboot wird angezeigt.

3. Aktivieren Sie das Kontrollkästchen **Wiederherstellungskonsole**.

4. Geben Sie die Anmeldedaten für das Endpoint Encryption Benutzerkonto ein.

5. Klicken Sie auf **Anmelden**.

   Die Wiederherstellungskonsole wird geöffnet.

Auf die Wiederherstellungskonsole von Windows aus zugreifen

Prozedur

1. Wechseln Sie unter Windows zum Installationsverzeichnis von Full Disk Encryption.

   Der Standardordner ist `C:\Program Files\Trend Micro\Full Disk Encryption\`.

2. Öffnen Sie `RecoveryConsole.exe`.

   Das Fenster **Wiederherstellungskonsole** wird angezeigt.

3. Geben Sie den Endpoint Encryption Benutzernamen und das Kennwort ein, und klicken Sie anschließend auf **Anmelden**.

Die Wiederherstellungskonsole wird mit der Seite **Festplatte entschlüsseln** geöffnet.

Full Disk Encryption in ein anderes Unternehmen migrieren

Eine PolicyServer Instanz kann mehrere Unternehmenskonfigurationen haben, die einen Geschäftsbereich oder eine Abteilung repräsentieren. Wenn Sie ein Gerät in ein neues Unternehmen verschieben, wird das Endpoint Encryption Gerät aus dem alten Unternehmen entfernt und dem neuen Unternehmen innerhalb derselben PolicyServer Instanz hinzugefügt. Möglicherweise muss der Full Disk Encryption Agent in ein neues Unternehmen verschoben werden, wenn der Mitarbeiter in eine andere Abteilung oder an einen anderen Standort versetzt wird.



Hinweis

Informationen über das Wechseln des PolicyServer, der den Full Disk Encryption Agent verwaltet, finden Sie unter *Full Disk Encryption PolicyServer wechseln auf Seite 6-49*.

Ein Wechsel des Unternehmens erfordert Zugriff auf die Full Disk Encryption Wiederherstellungskonsole. Weitere Informationen finden Sie unter *PolicyServer Einstellungen für Full Disk Encryption auf Seite 6-45*.



Warnung!

Wenn Sie das Unternehmen wechseln, müssen Sie die Richtlinien erneut konfigurieren und die Gruppen neu erstellen. Die gespeicherten Kennwörter, der Kennwortverlauf und die Audit-Protokolle werden gelöscht.

Prozedur

1. Klicken Sie auf **Netzwerk-Setup**.
2. Wählen Sie die Registerkarte **PolicyServer**.
3. Klicken Sie auf **Unternehmen wechseln**.

Das Fenster **Unternehmen wechseln** wird angezeigt.



Abbildung 6-4. Wiederherstellungskonsole – Unternehmen wechseln

4. Konfigurieren Sie die folgenden Optionen:

Option	Bezeichnung
Neuer Serverbenutzer	Geben Sie den Kontonamen eines Unternehmensadministrators oder den Benutzernamen eines Kontos an, das berechtigt ist, Installationen im Unternehmen oder der Gruppe im neuen PolicyServer durchzuführen.
Neues Benutzerkennwort	Geben Sie das Kennwort für den Unternehmensadministrator an.
Neue Serveradresse	Geben Sie die neue IP-Adresse oder den neuen Host-Namen für den PolicyServer ein.

OPTION	BEZEICHNUNG
Neues Unternehmen	Geben Sie das neue Unternehmen für den PolicyServer an.

5. Klicken Sie auf **Speichern**.

   Full Disk Encryption validiert die neuen Informationen für den PolicyServer.

6. Wenn die Bestätigungsmeldung angezeigt wird, klicken Sie auf **OK**.

Endpunkte auf einen neuen PolicyServer migrieren

In diesem Abschnitt wird beschrieben, wie Sie den PolicyServer wechseln, der die Richtlinien eines Endpoint Encryption Agent steuert. Sie müssen den Endpoint Encryption Agent möglicherweise auf einen anderen PolicyServer migrieren, wenn der Endpunkt in eine andere Abteilung verschoben wird, die von einer anderen PolicyServer Instanz verwaltet wird, oder wenn es Netzwerkfaktoren gibt, die es erforderlich machen, dass die IP-Adresse oder der Host-Name von PolicyServer geändert wird. Nach der Migration auf einen neuen PolicyServer wird der Endpunkt als neues Endpoint Encryption Gerät in der Datenbank des neuen PolicyServer registriert, und das zuvor registrierte Endpoint Encryption Gerät wird aus der Datenbank des alten PolicyServer entfernt.

Full Disk Encryption PolicyServer wechseln

Informationen darüber, warum Endpoint Encryption Agents den PolicyServer möglicherweise wechseln müssen, der die Richtlinien verwaltet, finden Sie unter *Endpunkte auf einen neuen PolicyServer migrieren auf Seite 6-49*.



Hinweis

Ein Wechsel des PolicyServer erfordert Zugriff auf die Full Disk Encryption Wiederherstellungskonsole. Weitere Informationen finden Sie unter *PolicyServer Einstellungen für Full Disk Encryption auf Seite 6-45*.

Prozedur

1. Klicken Sie auf der Full Disk Encryption Wiederherstellungskonsole auf die Registerkarte **PolicyServer**.
2. Klicken Sie auf **Server wechseln**.
3. Klicken Sie auf **Ja**, wenn die Warnmeldung angezeigt wird.
4. Geben Sie die neue Serveradresse ein.
5. Klicken Sie auf **Speichern**.

Den PolicyServer für die Encryption Management for Apple FileVault wechseln

Informationen darüber, warum Endpoint Encryption Agents den PolicyServer möglicherweise wechseln müssen, der die Richtlinien verwaltet, finden Sie unter *Endpunkte auf einen neuen PolicyServer migrieren auf Seite 6-49*.

Prozedur

1. Deinstallieren Sie den Agent der Encryption Management for Apple FileVault.

   Weitere Informationen finden Sie unter *Encryption Management for Apple FileVault deinstallieren auf Seite 6-54*.

2. Warten Sie, bis die Entschlüsselung der Festplatte abgeschlossen ist. Der Benutzer kann den Endpunkt ganz normal verwenden.
3. Entfernen Sie das Gerät vom alten PolicyServer.

   a. Melden Sie sich bei PolicyServer MMC an.

   b. Klicken Sie mit der rechten Maustaste auf das Endpoint Encryption Gerät, und wählen Sie anschließend **Gerät entfernen**.

   c. Klicken Sie zur Bestätigung auf **Ja**.

   Weitere Informationen über das Entfernen von Endpoint Encryption Geräten finden Sie im *Endpoint Encryption Administratorhandbuch*.

4. Folgen Sie den Installationsanweisungen für die Erstinstallation, um die Encryption Management for Apple FileVault unter *Den Agent der Encryption Management for Apple FileVault installieren auf Seite 6-21* Vergewissern Sie sich, dass Sie die Anmeldedaten für den neuen PolicyServer angeben.

5. Zur Bestätigung der Migration öffnen Sie entweder die Widgets "Control Manager Endpoint Encryption Devices" oder melden Sie sich an PolicyServer MMC an, der den neuen PolicyServer verwaltet.

Den PolicyServer für die Encryption Management for Microsoft BitLocker wechseln

Informationen darüber, warum Endpoint Encryption Agents den PolicyServer möglicherweise wechseln müssen, der die Richtlinien verwaltet, finden Sie unter *Endpunkte auf einen neuen PolicyServer migrieren auf Seite 6-49*.

Prozedur

1. Deinstallieren Sie den Agent der Encryption Management for Microsoft BitLocker.

   Weitere Informationen finden Sie unter *Encryption Management for Microsoft BitLocker deinstallieren auf Seite 6-55*.

2. Warten Sie, bis die Entschlüsselung der Festplatte abgeschlossen ist. Der Benutzer kann den Endpunkt ganz normal verwenden.

3. Entfernen Sie das Gerät vom alten PolicyServer.

   a. Melden Sie sich bei PolicyServer MMC an.

   b. Klicken Sie mit der rechten Maustaste auf das Endpoint Encryption Gerät, und wählen Sie anschließend **Gerät entfernen**.

   c. Klicken Sie zur Bestätigung auf **Ja**.

   Weitere Informationen über das Entfernen von Endpoint Encryption Geräten finden Sie im *Endpoint Encryption Administratorhandbuch*.

4. Folgen Sie den Installationsanweisungen für die Erstinstallation, um die Encryption Management for Microsoft BitLocker unter *Die Encryption Management for Microsoft*

*BitLocker Agent installieren auf Seite 6-18*Vergewissern Sie sich, dass Sie die Anmeldedaten für den neuen PolicyServer angeben.

5. Zur Bestätigung der Migration öffnen Sie entweder die Widgets "Control Manager Endpoint Encryption Devices" oder melden Sie sich an PolicyServer MMC an, der den neuen PolicyServer verwaltet.

Den File Encryption PolicyServer wechseln

Informationen darüber, warum Endpoint Encryption Agents den PolicyServer möglicherweise wechseln müssen, der die Richtlinien verwaltet, finden Sie unter *Endpunkte auf einen neuen PolicyServer migrieren auf Seite 6-49*.

Prozedur

1. Klicken Sie mit der rechten Maustaste auf das Task-Leistensymbol für File Encryption, und wählen Sie **Info über File Encryption**.
2. Klicken Sie auf **PolicyServer bearbeiten**.
3. Geben Sie die IP-Adresse oder den Host-Namen für den neuen PolicyServer an, und klicken Sie dann auf **OK**.

Deinstallation

Während eines Upgrades ist es bei einigen Endpoint Encryption Agents erforderlich, zuerst die alte Software für die Endpoint Encryption Agents manuell zu deinstallieren. Wenn die Software des Endpoint Encryption Agent Fehlfunktionen zeigt, lässt sich das Problem möglicherweise durch Deinstallieren und erneutes Installieren der Software für den Endpoint Encryption Agent lösen.

Im folgenden Abschnitt wird erklärt, wie Sie die Software für den Endpoint Encryption Agent deinstallieren oder mit OfficeScan den Deinstallationsbefehl gleichzeitig auf mehrere verwaltete Endpunkte verteilen.

Endpoint Encryption Agents manuell deinstallieren

Im folgenden Abschnitt wird beschrieben, wie Sie die Endpoint Encryption Agents mit dem Installationsprogramm manuell deinstallieren. Die Deinstallation der Software für Endpoint Encryption Agents ist möglicherweise erforderlich, um ein Problem zu lösen oder die Software für Endpoint Encryption Agents zu aktualisieren.

Full Disk Encryption deinstallieren

Während eines Upgrades ist es bei einigen Endpoint Encryption Agents erforderlich, zuerst die alte Software für die Endpoint Encryption Agents manuell zu deinstallieren. Wenn die Software des Endpoint Encryption Agent Fehlfunktionen zeigt, lässt sich das Problem möglicherweise durch Deinstallieren und erneutes Installieren der Software für den Endpoint Encryption Agent lösen.



Hinweis

Zur Deinstallation der Endpoint Encryption Agents muss das Benutzerkonto über die Berechtigung zur Deinstallation innerhalb der Gruppe oder Richtlinie, in der die Endpoint Encryption Geräte registriert sind, sowie über lokale Windows-Administratorrechte verfügen.



Tipp

Jeder Benutzer- oder Gruppenauthentifizierer kann das Deinstallationsprogramm unter Windows ausführen, wenn für die Richtlinie **Full Disk Encryption** > **Agent** > **Deinstallation durch Benutzer zulassen** = **Ja** festgelegt ist.

Prozedur

1. Melden Sie sich zuerst bei Full Disk Encryption Preboot und dann bei Windows an.

2. Wechseln Sie unter Windows zu `C:\Programme\Trend Micro\Full Disk Encryption` und führen Sie `TMFDEUninstall.exe` aus.



Hinweis

Wenn Sie eine Nachfrage von der **Benutzerkontensteuerung** erhalten, klicken Sie auf **Ja**.

Das Fenster zum Deinstallieren von Full Disk Encryption wird geöffnet.

3. Klicken Sie auf **Weiter**.

   Full Disk Encryption wird deinstalliert.

4. Klicken Sie auf **OK**, um die Entschlüsselung der Festplatte zu bestätigen.



Hinweis

Um den Status der Entschlüsselung anzuzeigen, öffnen Sie Full Disk Encryption von der Task-Leiste aus.

5. Wenn die Entschlüsselung abgeschlossen ist, klicken Sie auf **OK**.

6. Führen Sie `TMFDEUninstall.exe` erneut aus, um die Deinstallation abzuschließen.

7. Starten Sie das Gerät neu.



Hinweis

Der Gerätedatensatz wird nicht automatisch gelöscht. Er muss manuell aus PolicyServer entfernt werden.

Encryption Management for Apple FileVault deinstallieren

Wenn Sie den Agent der Encryption Management for Apple FileVault deinstallieren, benötigen Sie Zugriff auf das Terminalprogramm von Mac OS X.

Informationen zur Installation der Encryption Management for Apple FileVault finden Sie unter *Installation der Encryption Management for Apple FileVault auf Seite 6-20*.



Hinweis

Zur Deinstallation der Endpoint Encryption Agents muss das Benutzerkonto über die Berechtigung zur Deinstallation innerhalb der Gruppe oder Richtlinie, in der die Endpoint Encryption Geräte registriert sind, sowie über lokale Windows-Administratorrechte verfügen.



Tipp

Jeder Benutzer- oder Gruppenauthentifizierer kann das Deinstallationsprogramm unter Windows ausführen, wenn für die Richtlinie **Full Disk Encryption** > **Agent** > **Deinstallation durch Benutzer zulassen** = **Ja** festgelegt ist.

Prozedur

1. Navigieren Sie zu **Anwendungen** > **Dienstprogramme**, und doppelklicken Sie auf **Terminal**.

   Das Fenster "Terminal" wird angezeigt.

2. Geben Sie Folgendes ein: `cd /Library/Application Support/TrendMicro/FDEMM`

3. Geben Sie ein: `sudo ./Uninstaller`

   Der Agent wird im Hintergrund deinstalliert.

4. Starten Sie den Endpunkt neu, um die Deinstallation abzuschließen.

Encryption Management for Microsoft BitLocker deinstallieren

Deinstallieren Sie den Agent mit der Windows-Funktion **Programme und Features**. Encryption Management for Microsoft BitLocker.



Hinweis

Zur Deinstallation der Endpoint Encryption Agents muss das Benutzerkonto über die Berechtigung zur Deinstallation innerhalb der Gruppe oder Richtlinie, in der die Endpoint Encryption Geräte registriert sind, sowie über lokale Windows-Administratorrechte verfügen.



Tipp

Jeder Benutzer- oder Gruppenauthentifizierer kann das Deinstallationsprogramm unter Windows ausführen, wenn für die Richtlinie **Full Disk Encryption** > **Agent** > **Deinstallation durch Benutzer zulassen** = **Ja** festgelegt ist.

Prozedur

1. Navigieren Sie zu **Start** > **Einstellungen** > **Systemsteuerung** > **Programme und Features**

   Das Fenster **Programme und Features** wird angezeigt.

2. Wählen Sie Encryption Management for Microsoft BitLocker aus der Liste der installierten Programme.

3. Klicken Sie auf **Entfernen**.

4. Wenn die Meldung **Programme hinzufügen oder entfernen** angezeigt wird, klicken Sie zur Bestätigung auf **Ja**.

Die Deinstallation ist abgeschlossen, wenn das Programm aus der Liste entfernt wurde.

File Encryption deinstallieren

Deinstallieren Sie File Encryption mit der Windows-Funktion **Programme und Features**.



Hinweis

Zur Deinstallation der Endpoint Encryption Agents muss das Benutzerkonto über die Berechtigung zur Deinstallation innerhalb der Gruppe oder Richtlinie, in der die Endpoint Encryption Geräte registriert sind, sowie über lokale Windows-Administratorrechte verfügen.



Tipp

Jeder Benutzer- oder Gruppenauthentifizierer kann das Deinstallationsprogramm unter Windows ausführen, wenn für die Richtlinie **Full Disk Encryption** > **Agent** > **Deinstallation durch Benutzer zulassen** = **Ja** festgelegt ist.



Hinweis

- Legen Sie für **Richtlinien** > **File Encryption** > **Computer** > **Deinstallation durch Benutzer zulassen** die Option **Ja** fest, damit alle Benutzer oder Gruppenauthentifizierer das Deinstallationsprogramm unter Windows aufrufen dürfen.
- Speichern und schließen Sie alle Dokumente, bevor Sie die Deinstallation durchführen. Nachdem die Deinstallation abgeschlossen ist, müssen Sie einen Neustart durchführen.



Warnung!

Entschlüsseln Sie alle verschlüsselten Dateien, bevor Sie File Encryption deinstallieren. Anderenfalls sind diese nicht mehr lesbar.

Prozedur

1. Melden Sie sich bei File Encryption mit einem Konto an, das über die Berechtigung zum Deinstallieren von File Encryption verfügt.
2. Öffnen Sie das **Windows Startmenü** und navigieren Sie zu **Systemsteuerung** > **Programme** > **Programm deinstallieren**.
3. Wählen Sie "File Encryption" aus der Liste, und klicken Sie anschließend auf **Deinstallieren**.

Mit OfficeScan Endpoint Encryption Agents deinstallieren

Während eines Upgrades ist es bei einigen Endpoint Encryption Agents erforderlich, zuerst die alte Software für die Endpoint Encryption Agents manuell zu deinstallieren. Wenn die Software des Endpoint Encryption Agent Fehlfunktionen zeigt, lässt sich das Problem möglicherweise durch Deinstallieren und erneutes Installieren der Software für den Endpoint Encryption Agent lösen. Dieses Verfahren erklärt die Deinstallation von Endpoint Encryption Agents mit dem Plug-in für das OfficeScan Endpoint Encryption Verteilungstool.

Prozedur

1. Wählen Sie das Endpoint Encryption Gerät.

   
   Hinweis

   Wenn Sie mehrere Endpoint Encryption Geräte auswählen möchten, halten Sie die UMSCHALTTASTE gedrückt, und wählen Sie die entsprechenden Endpunkte.

2. Klicken Sie auf **Deinstallieren**, und wählen Sie den entsprechenden Endpoint Encryption Agent aus dem Listenfeld.

3. Klicken Sie auf **OK**, um die Verteilung zu bestätigen.

   Der Deinstallationsbefehl für den Endpoint Encryption Agent wird verteilt.

4. Die Deinstallation des Endpoint Encryption Agent ist abgeschlossen, wenn OfficeScan die Bestätigungsmeldung anzeigt.

   
   Hinweis

   Alle zukünftigen Verteilungsbefehle schlagen fehl, wenn das Endpoint Encryption Gerät nicht neu gestartet wird, nachdem der Deinstallationsbefehl aufgerufen und abgeschlossen wurde. Wenn die Deinstallation nicht abgeschlossen werden kann, führen Sie die manuelle Deinstallation durch, siehe *Deinstallation auf Seite 6-52*.

Bei vollständiger Deinstallation wird der Endpoint Encryption Agent entfernt, und der Produktordner wird auf dem Endpunkt gelöscht.



Kapitel 7

Integration von OfficeScan

Im Folgenden wird beschrieben, wie das OfficeScan Plug-in für das Endpoint Encryption Verteilungstool zur Verteilung von Endpoint Encryption in Unternehmen mit Endpunkten, die von OfficeScan verwaltet werden, verwendet wird.

Es werden folgende Themen behandelt:

Info über Trend Micro OfficeScan Integration

OfficeScan schützt Unternehmensnetzwerke vor Malware, Netzwerkviren, webbasierten Bedrohungen, Spyware und kombinierten Bedrohungen. OfficeScan ist eine integrierte Lösung und besteht aus einem Agent am Endpunkt sowie einem Serverprogramm, das alle Agents verwaltet. Der Agent überwacht den Endpunkt und sendet dessen Sicherheitsstatus an den Server. Über die webbasierte Management-Konsole vereinfacht der Server das Festlegen koordinierter Sicherheitsrichtlinien und verteilt Updates an alle Agents.



Hinweis

Informationen über OfficeScan finden Sie in der Begleitdokumentation unter:

http://docs.trendmicro.com/de-de/enterprise/officescan.aspx

Mit dem Plug-in für das OfficeScan Endpoint Encryption Verteilungstool können Sie die Endpoint Encryption Agents auf verwaltete OfficeScan Endpunkte verteilen. Sie können Endpunkte auf Grundlage bestimmter Kriterien auswählen und den Status der Verteilung anzeigen. Nachdem das Plug-in für das Endpoint Encryption Verteilungstool die Software für den Endpoint Encryption Agent verteilt hat, führt der Endpoint Encryption Agent eine Synchronisierung mit PolicyServer unter Verwendung der Einstellungen durch, die im Plug-in angegeben wurden. OfficeScan verwaltet keine Endpoint Encryption Richtlinien. Der OfficeScan Agent und der Endpoint Encryption Agent befinden sich unabhängig voneinander auf demselben Endpunkt.

In der folgenden Darstellung wird illustriert, wie Sie Endpoint Encryption zum ersten Mal auf Endpunkte verteilen, die von OfficeScan verwaltet werden. In OfficeScan

Installationen können Administratoren PolicyServer entweder mit Control Manager oder PolicyServer MMC verwalten.

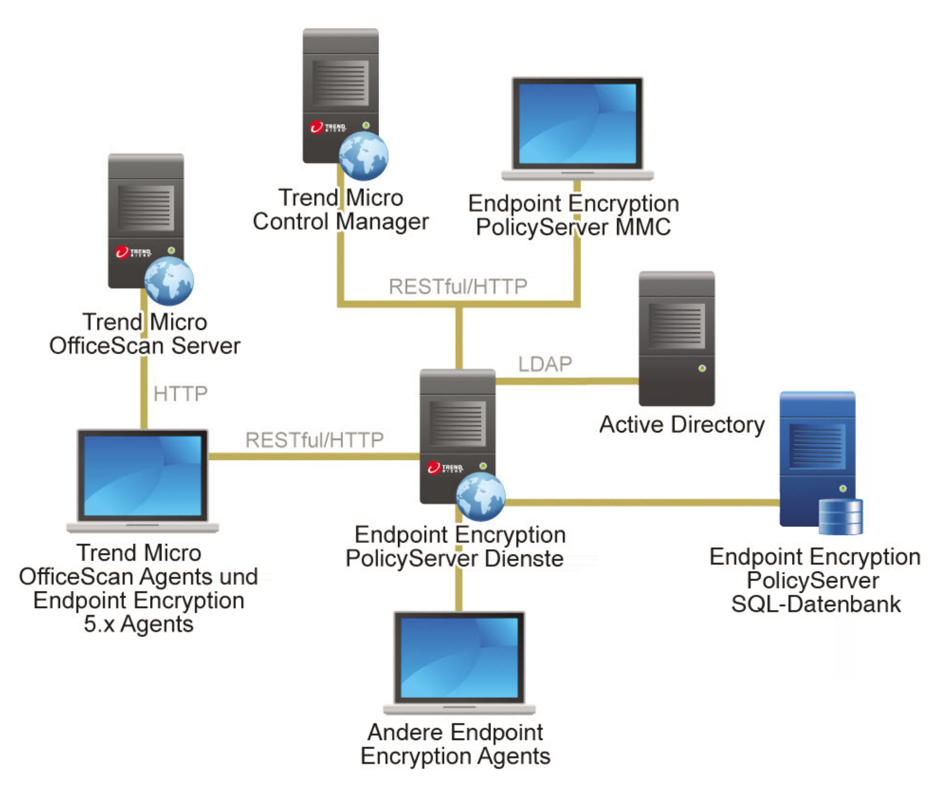


ABBILDUNG 7-1. Verteilung der OfficeScan Integration

OfficeScan installieren

Informationen zur Installation und Konfiguration von OfficeScan finden Sie in der Dokumentation, die Sie unter der folgenden Adresse herunterladen können:

http://docs.trendmicro.com/de-de/enterprise/officescan.aspx

Informationen zu den Installations- und Konfigurationsoptionen des OfficeScan Endpoint Encryption Verteilungstools vor der Verteilung der Endpoint Encryption Agents finden Sie im *Endpoint Encryption Installations- und Migrationshandbuch*.

Info über den Plug-in Manager

OfficeScan umfasst ein Framework mit der Bezeichnung Plug-in Manager, das neue Lösungen in die bestehende OfficeScan Umgebung integriert. Um die Verwaltung dieser Lösungen zu vereinfachen, stellt Plug-in Manager die Daten dieser Lösungen in Form von Widgets übersichtlich dar.



Hinweis

Keine der Plug-in-Lösungen unterstützt zurzeit IPv6. Der Server kann diese Lösungen zwar herunterladen, er kann sie aber nicht auf reine IPv6 Endpoint Encryption Agents oder reine IPv6-Hosts verteilen.

Plug-in Manager liefert zwei verschiedene Lösungen:

- **Native Produktfunktionen**

  Einige native OfficeScan Funktionen werden über Plug-in Manager separat lizenziert und aktiviert. In dieser Version fallen zwei Funktionen unter diese Kategorie, nämlich **Trend Micro Virtual Desktop Support** und **OfficeScan Datentschutz**.

- **Plug-in-Programme**

  Plug-in-Programme sind nicht Teil des OfficeScan Programms. Die Plug-in-Programme haben separate Lizenzen und Management-Konsolen. Greifen Sie auf die Management-Konsolen über die OfficeScan Webkonsole zu. Beispiele für Plug-in-Programme sind **Intrusion Defense Firewall**, **Trend Micro Security (für Mac)** und **Trend Micro Mobile Security**.

Diese Dokumente geben einen allgemeinen Überblick über Installation und Verwaltung von Plug-in-Programmen und erklären die in Widgets dargestellten Informationen über die Plug-in-Programme. Die Dokumentation enthält außerdem ausführliche Hinweise zur Konfiguration und Verwaltung des jeweiligen Plug-in-Programms.

Installation des Endpoint Encryption Verteilungstools

Plug-in-Programme werden auf der **Plug-in Manager** Konsole angezeigt. Auf der Konsole können Sie die Programme herunterladen, installieren und verwalten. Der Plug-In Manager lädt das Installationspaket für das Plug-In-Programm vom Trend Micro ActiveUpdate Server oder einer benutzerdefinierten Update-Quelle herunter, falls eine solche korrekt erstellt wurde. Zum Herunterladen des Pakets vom ActiveUpdate Server ist eine Internet-Verbindung erforderlich.

Wenn der Plug-in Manager ein Installationspaket herunterlädt oder die Installation startet, deaktiviert er vorübergehend andere Plug-in-Programmfunktionen wie Downloads, Installationen und Upgrades.

Der Plug-in Manager unterstützt keine Installation oder Verwaltung von Plug-in-Programmen über die Single-Sign-On-Funktion von Trend Micro Control Manager.

Endpoint Encryption Verteilungstool installieren

Prozedur

1. Öffnen Sie die OfficeScan Webkonsole und klicken Sie im Hauptmenü auf **Plug-in Manager**.
2. Navigieren Sie im Plug-in Manager Fenster zum Abschnitt **"Plug-in-Programm"**, und klicken Sie auf **"Download"**.

   Die Größe des Plug-in-Programmpakets wird neben der Schaltfläche **Download** angezeigt. .

   Überwachen Sie den Fortschritt oder navigieren Sie während des Downloads aus dem Fenster heraus.

   Hinweis

   Wenn OfficeScan beim Herunterladen oder Installieren des Pakets Probleme erkennt, überprüfen Sie die Server-Update-Protokolle auf der OfficeScan Webkonsole. Klicken Sie im Hauptmenü auf **Protokolle** > **Server-Update**.

3. Klicken Sie auf **Jetzt installieren** oder **Später installieren**.

   - Nachdem Sie auf **Jetzt installieren** geklickt haben, wird mit der Installation begonnen, und das Fenster mit dem Installationsfortschritt wird angezeigt.
   - Nachdem Sie auf **Später installieren** geklickt haben, wird das Fenster **Plug-in Manager** angezeigt.

     Installieren Sie das Plug-in-Programm, indem Sie auf die Schaltfläche **Installieren** klicken, die sich im Abschnitt des Plug-in-Programms im Fenster **Plug-in Manager** befindet.

   Das Fenster **Trend Micro Endbenutzer-Lizenzvereinbarung** wird angezeigt.



Hinweis

Nicht alle Plug-in-Programme erfordern dieses Fenster. Wenn dieses Fenster nicht angezeigt wird, beginnt die Installation des Plug-in-Programms.

4. Klicken Sie auf **Zustimmen**, um das Plug-in-Programm zu installieren.

   Überwachen Sie den Fortschritt, oder navigieren Sie während der Installation aus dem Fenster heraus.



Hinweis

Wenn OfficeScan beim Herunterladen oder Installieren des Pakets Probleme erkennt, überprüfen Sie die Server-Update-Protokolle auf der OfficeScan Webkonsole. Klicken Sie im Hauptmenü auf **Protokolle** > **Server-Update**.

Nach der Installation wird die aktuelle Version des Plug-in-Programms im Fenster **Plug-in Manager** angezeigt.

Verwaltung der Plug-in-Programme

Konfigurieren Sie die Einstellungen und führen Sie programmbezogene Aufgaben über die Management-Konsole des Plug-in-Programms durch, auf die Sie über die OfficeScan Webkonsole zugreifen können. Zu den Aufgaben gehören das Aktivieren des

Programms und die mögliche Verteilung des Plug-in-Programm-Agents an die Endpunkte. Die Dokumentation enthält außerdem ausführliche Hinweise zur Konfiguration und Verwaltung des jeweiligen Plug-in-Programms.

Endpoint Encryption Verteilungstool verwalten

Prozedur

1. Öffnen Sie die OfficeScan Webkonsole und klicken Sie im Hauptmenü auf **Plug-in Manager**.

2. Navigieren Sie im **Plug-in Manager** Fenster zum Abschnitt für Plug-in-Programme, und klicken Sie auf **Programm verwalten**.

Plug-in-Programme verwenden

In diesem Abschnitt wird beschrieben, wie Sie das Plug-in-Programm für das OfficeScan Endpoint Encryption Verteilungstool installieren und verwalten.

Verwaltung der Plug-in-Programme

Konfigurieren Sie die Einstellungen und führen Sie programmbezogene Aufgaben über die Management-Konsole des Plug-in-Programms durch, auf die Sie über die OfficeScan Webkonsole zugreifen können. Zu den Aufgaben gehören das Aktivieren des Programms und die mögliche Verteilung des Plug-in-Programm-Agents an die Endpunkte. Die Dokumentation enthält außerdem ausführliche Hinweise zur Konfiguration und Verwaltung des jeweiligen Plug-in-Programms.

Endpoint Encryption Verteilungstool verwalten

Prozedur

1. Öffnen Sie die OfficeScan Webkonsole und klicken Sie im Hauptmenü auf **Plug-in Manager**.

2. Navigieren Sie im **Plug-in Manager** Fenster zum Abschnitt für Plug-in-Programme, und klicken Sie auf **Programm verwalten**.

Upgrades für das Endpoint Encryption Verteilungstool

Jede neue Version eines installierten Plug-in-Programms wird auf der Plug-in Manager-Konsole angezeigt. Laden Sie das Paket herunter, und aktualisieren Sie das Plug-in-Programm auf der Konsole. Der Plug-in Manager lädt das Paket vom Trend Micro ActiveUpdate Server oder einer definierten Update-Quelle herunter, falls eine solche ordnungsgemäß erstellt wurde. Zum Herunterladen des Pakets vom ActiveUpdate Server ist eine Internet-Verbindung erforderlich.

Wenn der Plug-in Manager ein Installationspaket herunterlädt oder ein Upgrade startet, deaktiviert er vorübergehend andere Plug-in-Programmfunktionen wie Downloads, Installationen und Upgrades.

Der Plug-in Manager unterstützt kein Upgrade des Plug-in-Programms über die Single-Sign-On-Funktion von Trend Micro Control Manager.

Endpoint Encryption Verteilungstool aktualisieren

Prozedur

1. Öffnen Sie die OfficeScan Webkonsole und klicken Sie im Hauptmenü auf **Plug-in Manager**.

2. Navigieren Sie im Plug-in Manager Fenster zum Abschnitt **"Plug-in-Programm"**, und klicken Sie auf **"Download"**.

   Die Größe des Upgrade-Pakets erscheint neben der Schaltfläche **Download**.

3. Verfolgen Sie den Download-Fortschritt.

   Wenn Sie während des Download-Vorgangs das Fenster verlassen, wirkt sich dies nicht auf das Upgrade aus.



Hinweis

Wenn OfficeScan beim Herunterladen oder Installieren des Pakets Probleme erkennt, überprüfen Sie die Server-Update-Protokolle auf der OfficeScan Webkonsole. Klicken Sie im Hauptmenü auf **Protokolle** > **Server-Update**.

4. Nach dem Download des Pakets wird ein neues Fenster angezeigt:

Nach dem Upgrade muss der Plug-in Manager Dienst möglicherweise neu gestartet werden. Das **Plug-in Manager** Fenster ist dann vorübergehend nicht verfügbar. Sobald das Fenster wieder verfügbar ist, wird die aktuelle Version des Plug-in-Programms angezeigt.

Deinstallation des Endpoint Encryption Verteilungstools

Es gibt folgende Möglichkeiten, ein Plug-in-Programm zu deinstallieren:

- Deinstallieren Sie das Plug-in-Programm über die Plug-in Manager-Konsole.
- Deinstallieren Sie den OfficeScan Server. Dabei werden der Plug-in Manager und alle installierten Plug-in-Programme ebenfalls deinstalliert. Informationen über die Deinstallation des OfficeScan Servers finden Sie im *OfficeScan Installations- und Upgrade-Handbuch*.

Endpoint Encryption Verteilungstool über die Plug-in Manager Konsole deinstallieren

---

Prozedur

1. Öffnen Sie die OfficeScan Webkonsole und klicken Sie im Hauptmenü auf **Plug-in Manager**.
2. Navigieren Sie im **Plug-in Manager** Fenster zum Abschnitt für Plug-in-Programme, und klicken Sie auf **Deinstallieren**.
3. Überwachen Sie den Fortschritt der Deinstallation, oder navigieren Sie während der Deinstallation aus dem Fenster heraus.
4. Aktualisieren Sie das Fenster **Plug-in Manager** nach der Deinstallation.

Das Plug-in-Programm steht wieder zur Installation zur Verfügung.

Agent-Hierarchie verwalten

Die OfficeScan Agent-Hierarchie

In der OfficeScan Agent-Hierarchie werden alle Agents – in OfficeScan Domänen gruppiert – angezeigt, die gegenwärtig vom Server verwaltet werden. Agents werden in Domänen gruppiert, so dass Sie für alle Domänenmitglieder gleichzeitig dieselbe Konfiguration festlegen, verwalten und übernehmen können.

Spezifische Aufgaben in der Agent-Hierarchie

Die Agent-Hierarchie wird angezeigt, wenn Sie bestimmte Fenster auf der Webkonsole öffnen. Oberhalb der Agent-Hierarchie befinden sich Menübefehle, die sich auf das gerade geöffnete Fenster beziehen. Mit Hilfe dieser Menübefehle können Sie bestimmte Aufgaben ausführen, z. B. die Konfiguration der Agent-Einstellungen oder die Einleitung von Agent-Aufgaben. Um eine dieser Aufgaben durchzuführen, wählen Sie zunächst ein Ziel für die Aufgabe, und wählen Sie anschließend einen Menübefehl.

Die Agent-Hierarchie bietet den Zugriff auf die folgenden Funktionen:

- **Nach Endpunkten suchen:** Suchen Sie nach bestimmten Endpunkten, indem Sie Suchkriterien in das Textfeld eingeben.
- **Mit OfficeScan synchronisieren**: Synchronisieren Sie die Agent-Hierarchie des Plug-in-Programms mit der Agent-Hierarchie von OfficeScan Server. Weitere Informationen finden Sie unter *Agent-Hierarchie synchronisieren auf Seite 7-11*.
- **Server-Einstellungen verteilen**: Zeigt das Fenster **Server-Einstellungen verteilen** an. Weitere Informationen finden Sie unter *Servereinstellungen verteilen auf Seite 7-11*.

Administratoren können auch die Agent-Hierarchie manuell durchsuchen, um Endpunkte oder Domänen zu finden. Die computerspezifischen Informationen werden in der Tabelle rechts angezeigt.

Agent-Hierarchie synchronisieren

Bevor das Plug-in-Programm die Einstellungen an die Agents verteilen kann, müssen Administratoren die Agent-Hierarchie mit dem OfficeScan Server synchronisieren.

Prozedur

1. Öffnen Sie die Plug-in-Konsole.
2. Klicken Sie im Fenster **Client-Verwaltung** auf **Mit OfficeScan synchronisieren**.

   Ein Bestätigungsfenster wird angezeigt.
3. Warten Sie, bis der Synchronisierungsvorgang abgeschlossen ist.
4. Klicken Sie auf **Schließen**, um zum Fenster **Client-Verwaltung** zurückzukehren.

Servereinstellungen verteilen

Sie können die Einstellungen für PolicyServer konfigurieren und verteilen, um die Kommunikation zwischen den Agents und PolicyServer sicherzustellen.

Prozedur

1. Öffnen Sie die Plug-in-Programmkonsole.
2. Klicken Sie auf die Registerkarte **PolicyServer Einstellungen**.
3. Geben Sie die folgenden Details an:

OPTION	BEZEICHNUNG
Servername:	Geben Sie die IP-Adresse oder den Host-Namen für den PolicyServer ein.
Port	Geben Sie die Portnummer an, die der PolicyServer Instanz zugewiesen wurde.
Unternehmen	Geben Sie das PolicyServer Unternehmen an. Nur ein Unternehmen wird unterstützt.
Benutzername	Geben Sie den Benutzernamen für den Unternehmensadministrator an.
Kennwort	Geben Sie das Kennwort für den Unternehmensadministrator an.

4. Klicken Sie auf **Speichern**.

   Eine Bestätigungsmeldung wird angezeigt. Warten Sie, bis die Verbindung mit dem Server erstellt wurde.

Verteilung von Endpoint Encryption Agents

In diesem Abschnitt wird beschrieben, wie Sie mit dem Plug-in für das Endpoint Encryption Verteilungstool die Befehle zur Installation und Deinstallation von Agents einleiten.

Die folgende Darstellung zeigt das Endpoint Encryption Verteilungstool-Fenster **Client-Verwaltung**.

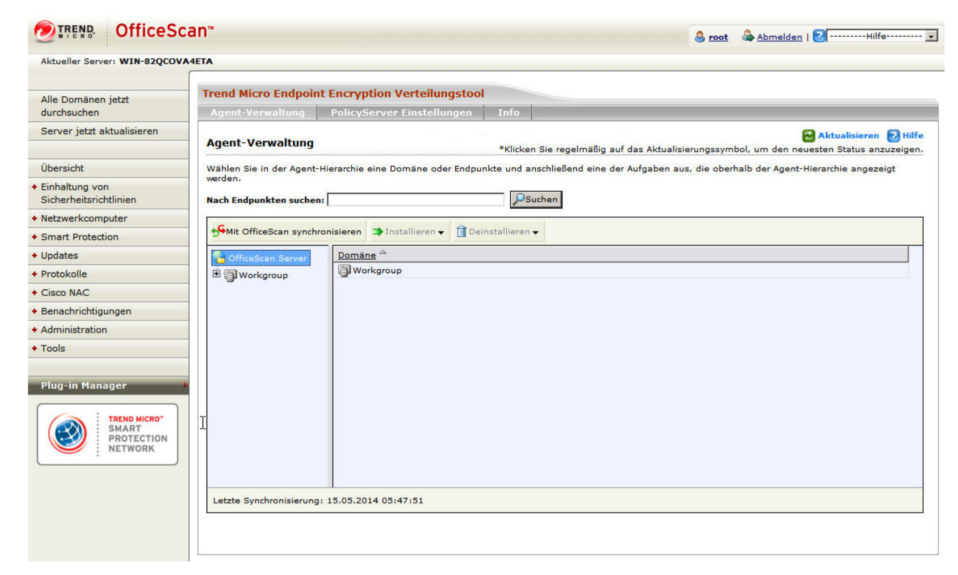


ABBILDUNG 7-2. Endpoint Encryption - Verteilungstool

Agent mit OfficeScan verteilen

Vergewissern Sie sich vor der Verteilung von Agents, dass die Endpunkte die minimalen Systemvoraussetzungen erfüllen. Weitere Informationen finden Sie unter *Systemvoraussetzungen auf Seite 2-1*.

Prozedur

1. Wählen Sie den Endpunkt in der Client-Hierarchie aus.



Hinweis

Wenn Sie mehrere Endpunkte auswählen möchten, halten Sie die STRG-Taste gedrückt, und wählen Sie die entsprechenden Endpunkte aus.

2. Klicken Sie auf **Installieren**, und wählen Sie anschließend eine der folgenden Optionen:

OPTION	BEZEICHNUNG
Full Disk Encryption	Wählen Sie die entsprechenden Full Disk Encryption Agents. • Wählen Sie den Full Disk Encryption Agent, um alle Funktionen zu verteilen, einschließlich Preboot-Authentifizierung, aller Richtlinien, Benachrichtigungen und Aktionen für Geräte. • Wählen Sie den Agent für die Encryption Management for Microsoft BitLocker, um die Festplattenverschlüsselung von Microsoft BitLocker zu aktivieren. Dabei werden nur begrenzte Richtlinien und Aktionen für Geräte verteilt. **Hinweis** Es ist nicht möglich, den Agent der Encryption Management for Apple FileVault mit dem Endpoint Encryption Verteilungstool Plug-in zu verteilen.
File Encryption	Bei der Verteilung von File Encryption Agent sind alle Funktionen und Richtlinien enthalten.

3. Klicken Sie auf **Verteilen**.

4. Wenn eine Meldung angezeigt wird, klicken Sie auf **OK**, um die Verteilung zu bestätigen.

Der Befehl für die Agent-Verteilung wird eingeleitet. Bei Erfolg wird die Aufforderung angezeigt, den ausgewählten Endpunkt neu zu starten.

Agent-Verteilung bestätigen

Mit dieser Aufgabe wird erklärt, wie Sie bestätigen, dass die Installation von Endpoint Encryption Agent auf dem Endpunkt richtig initialisiert wurde.

Prozedur

1. Führen Sie *Agent mit OfficeScan verteilen auf Seite 7-13* durch.

2. Melden Sie sich am ausgewählten Endpoint Encryption Gerät an.

3. Wählen Sie eine der folgenden Optionen:

   - Um den Status der Verteilung anzuzeigen, öffnen Sie die Protokolldateien unter:

     Client-Endpunkt

     `C:\TMEE_Deploy_Client.log`

     Server-Endpunkt

     `C:\TMEE_Deploy_Server_Inst.log`

   - Führen Sie den Task-Manager aus, und suchen Sie nach einem der Dienste unter *Endpoint Encryption Agent-Dienste auf Seite 7-15*.

4. Sobald die Verteilung der Endpoint Encryption Agents beendet ist, starten Sie den Endpunkt neu, um die Installation abzuschließen.

Endpoint Encryption Agent-Dienste

In der folgenden Tabelle werden die Dienste beschrieben, die ausgeführt werden, wenn der Endpoint Encryption Agent auf dem Endpunkt initiiert wird. Anhand dieser Informationen können Sie überprüfen, ob der Agent erfolgreich installiert wurde und ordnungsgemäß funktioniert.



Hinweis

Weitere Informationen zu Endpoint Encryption Diensten finden Sie unter *Endpoint Encryption Dienste auf Seite D-1*.

Dienst	Status
`FEService.exe`	Der File Encryption Agent wird ausgeführt.
`TMFDE.exe`	Der Full Disk Encryption Agent wird ausgeführt.

DIENST	STATUS
`TMFDEForBitLocker.exe`	Die Encryption Management for Microsoft BitLocker Agent wird ausgeführt.

Statusangaben zur Verteilung von Endpoint Encryption Agents

In der folgenden Tabelle werden die Statusangaben von OfficeScan beschrieben, die auf der Konsole des Plug-ins für das Endpoint Encryption Verteilungstool nach der Initiierung des Verteilungsbefehls angezeigt werden. Anhand dieser Informationen können Sie ermitteln, ob während der Installation oder Deinstallation des Agents ein Problem aufgetreten ist.

TABELLE 7-1. Statusangaben zur Agent-Installation

STATUS	NACHRICHT	BESCHREIBUNG
Wird ausgeführt	Wird ausgeführt: Agent-Verteilung	OfficeScan versucht, eine Kommunikation mit dem verwalteten Endpunkt aufzubauen, den Endpoint Encryption Agent zu installieren und dann eine Verbindung mit PolicyServer zu erstellen.
Erfolgreich	Erfolgreiche Verteilung des Agent	Der Endpoint Encryption Agent wurde erfolgreich installiert und konnte die Kommunikation mit OfficeScan und PolicyServer aufbauen.
Fehlgeschlagen	Erfolglose Verteilung des Agent	Die Verteilung des Endpoint Encryption Agent konnte nicht abgeschlossen werden. Ermitteln Sie anhand der Protokolle, warum der verwaltete Endpunkt nicht mit dem ausgewählten Endpoint Encryption Agent aktualisiert werden konnte.

Status	Nachricht	Beschreibung
Neustart erforderlich	Erfolgreiche Verteilung des Agent Herunterfahren/Neustart erforderlich.	Beim Full Disk Encryption Agent ist ein Neustart erforderlich, um die Installation abzuschließen. Der Status wird erst aktualisiert, nachdem sich der Benutzer bei PolicyServer Preboot angemeldet hat.
Zeitüberschreitung	Zeitüberschreitung: Agent-Verteilung	Der Zeitraum für die Zeitüberschreitung beträgt 30 Minuten. Initiieren Sie nach einer Zeitüberschreitung einen neuen Verteilungsbefehl.

Tabelle 7-2. Statusangaben zur Agent-Deinstallation

Status	Nachricht	Beschreibung
Wird ausgeführt	Anforderung wird ausgeführt: Agent-Verteilung	OfficeScan versucht, mit dem verwalteten Endpunkt zu kommunizieren und die Agent-Software zu deinstallieren. Die Deinstallation kann erst starten, nachdem der verwaltete Endpunkt geantwortet hat.
Erfolgreich	Erfolgreiche Deinstallation des Agent	Der Endpoint Encryption Agent wurde erfolgreich deinstalliert und konnte die Kommunikation mit OfficeScan und PolicyServer aufbauen. Nach der Deinstallation wird das Endpoint Encryption Gerät von PolicyServer entfernt.
Fehlgeschlagen	Erfolglose Deinstallation des Agent	Für die Anforderung zur Deinstallation des Endpoint Encryption Agent konnte keine Verbindung erstellt werden. Ermitteln Sie anhand der Protokolle, warum auf dem verwalteten Endpunkt Endpoint Encryption nicht deinstalliert werden konnte.

STATUS	NACHRICHT	BESCHREIBUNG
Neustart erforderlich	Erfolgreiche Deinstallation des Agent Herunterfahren/Neustart erforderlich.	Einige Endpoint Encryption Agents müssen neu gestartet werden, damit die Deinstallation abgeschlossen werden kann.
Zeitüberschreitung	Zeitüberschreitung der Anforderung: Agent deinstallieren	Der Zeitraum für die Zeitüberschreitung beträgt 30 Minuten. Initiieren Sie nach einer Zeitüberschreitung einen neuen Deinstallationsbefehl.

Fehlercodes bei der Installation von Endpoint Encryption Agents

In der folgenden Tabelle werden die Fehlercodes für Fehler bei der Installation von Endpoint Encryption Agents beschrieben. Anhand dieser Tabelle können Sie das Problem verstehen und eine Lösung für den jeweiligen Installationsfehler finden.



Hinweis

Vergewissern Sie sich vor der Verteilung der Endpoint Encryption Agents, dass der Endpunkt die minimalen Systemvoraussetzungen erfüllt. Microsoft .NET Framework 2.0 SP1 oder höher ist erforderlich. Informationen zu den Systemvoraussetzungen finden Sie im *Endpoint Encryption Installations- und Migrationshandbuch*.

TABELLE 7-3. Fehlercodes im Zusammenhang mit der Installation

AGENT	FEHLERCODE	PROBLEM UND LÖSUNG
File Encryption	1603	Der Endpoint Encryption Agent kann nicht installiert werden. Möglicherweise ist eine erforderliche Ressource nicht verfügbar. Starten Sie den Endpunkt neu, und wiederholen Sie die Installation. Falls das Problem weiterhin besteht, wenden Sie sich an den Trend Micro Support.
Full Disk Encryption	-3	Der Benutzername oder das Kennwort ist ungültig. Überprüfen Sie die Anmeldedaten, und melden Sie sich erneut am PolicyServer an.
	-6	Der Endpoint Encryption Agent kann nicht installiert werden. Möglicherweise ist eine erforderliche Ressource nicht verfügbar. Starten Sie den Endpunkt neu, und wiederholen Sie die Installation. Falls das Problem weiterhin besteht, wenden Sie sich an den Trend Micro Support.
	-13	Der Endpunkt erfüllt nicht die minimalen Systemvoraussetzungen. Rüsten Sie den Arbeitsspeicher oder den Festplattenspeicherplatz auf, und wiederholen Sie die Installation des Agent.

AGENT	FEHLERCODE	PROBLEM UND LÖSUNG
Encryption Management for Microsoft BitLocker	1603	Der Endpoint Encryption Agent kann nicht installiert werden. Möglicherweise ist eine erforderliche Ressource nicht verfügbar. Starten Sie den Endpunkt neu, und wiederholen Sie die Installation. Falls das Problem weiterhin besteht, wenden Sie sich an den Trend Micro Support.
	-13	Der Endpoint Encryption Agent kann nicht installiert werden. Microsoft BitLocker erfordert das TPM-Sicherheitsgerät (Trusted Platform Module). Der Endpunkt unterstützt entweder TPM nicht, oder TPM ist nicht im BIOS aktiviert, oder TPM ist durch einen anderen angemeldeten Benutzer gesperrt. Aktivieren Sie TPM im BIOS, oder wenden Sie sich an den Systemadministrator.
	-14	Der Endpoint Encryption Agent kann nicht installiert werden. Das Betriebssystem wird nicht unterstützt. Installieren Sie eines der folgenden unterstützten Betriebssysteme, und versuchen Sie es anschließend erneut: • Windows 7, 32 Bit oder 64 Bit, Ultimate oder Enterprise Edition • Windows 8, 32 Bit oder 64 Bit, Professional oder Enterprise Edition
	-15	Full Disk Encryption ist bereits installiert.
	-16	Der Endpoint Encryption Agent kann nicht installiert werden. Der Endpunkt ist bereits verschlüsselt.

Mit OfficeScan Endpoint Encryption Agents deinstallieren

Während eines Upgrades ist es bei einigen Endpoint Encryption Agents erforderlich, zuerst die alte Software für die Endpoint Encryption Agents manuell zu deinstallieren. Wenn die Software des Endpoint Encryption Agent Fehlfunktionen zeigt, lässt sich das Problem möglicherweise durch Deinstallieren und erneutes Installieren der Software für den Endpoint Encryption Agent lösen. Dieses Verfahren erklärt die Deinstallation von Endpoint Encryption Agents mit dem Plug-in für das OfficeScan Endpoint Encryption Verteilungstool.

Prozedur

1. Wählen Sie das Endpoint Encryption Gerät.



Hinweis

Wenn Sie mehrere Endpoint Encryption Geräte auswählen möchten, halten Sie die UMSCHALTTASTE gedrückt, und wählen Sie die entsprechenden Endpunkte.

2. Klicken Sie auf **Deinstallieren**, und wählen Sie den entsprechenden Endpoint Encryption Agent aus dem Listenfeld.

3. Klicken Sie auf **OK**, um die Verteilung zu bestätigen.

   Der Deinstallationsbefehl für den Endpoint Encryption Agent wird verteilt.

4. Die Deinstallation des Endpoint Encryption Agent ist abgeschlossen, wenn OfficeScan die Bestätigungsmeldung anzeigt.



Hinweis

Alle zukünftigen Verteilungsbefehle schlagen fehl, wenn das Endpoint Encryption Gerät nicht neu gestartet wird, nachdem der Deinstallationsbefehl aufgerufen und abgeschlossen wurde. Wenn die Deinstallation nicht abgeschlossen werden kann, führen Sie die manuelle Deinstallation durch, siehe *Deinstallation auf Seite 6-52*.

Bei vollständiger Deinstallation wird der Endpoint Encryption Agent entfernt, und der Produktordner wird auf dem Endpunkt gelöscht.



Kapitel 8

Wartung und technischer Support

In den folgenden Themen wird der Wartungsvertrag erläutert und beschrieben, wie Sie online nach Lösungen suchen, das Support-Portal verwenden, mit Trend Micro Kontakt aufnehmen und zusätzliche Ressourcen finden.

Es werden folgende Themen behandelt:

Wartungsvertrag

Ein Wartungsvertrag zwischen Ihrem Unternehmen und Trend Micro regelt, in welchem Umfang Sie nach Zahlung der entsprechenden Gebühren Anrecht auf den Erhalt von technischem Support und Produkt-Updates haben. Beim Kauf eines Trend Micro Produkts enthält die Lizenzvereinbarung, die Sie mit dem Produkt erhalten, die Bestimmungen des Wartungsvertrags für dieses Produkt.

Eine Lizenz für die Trend Micro Software enthält üblicherweise das Recht auf Produkt- und Pattern-Datei-Updates und grundlegenden technischen Support (Wartung) für ein (1) Jahr ab Kaufdatum. Nach Ablauf dieser Frist muss der Wartungsvertrag jährlich zu den jeweils aktuellen Wartungsgebühren von Trend Micro verlängert werden.

Auch nach Ablauf des Wartungsvertrags kann eine Virensuche durchgeführt werden. Allerdings können Sie das Produkt nicht mehr aktualisieren, auch nicht manuell. Ebenso haben Sie keinen Anspruch mehr auf technischen Support von Trend Micro.

Normalerweise werden Sie neunzig (90) Tage vor Ablauf des Wartungsvertrags darauf hingewiesen, dass der Vertrag in Kürze abläuft. Sie können den Wartungsvertrag aktualisieren, indem Sie eine Verlängerung erwerben. Dies ist über Ihren Händler, den Trend Micro Vertrieb oder den Trend Micro Online-Registrierungsserver möglich. Sie erreichen ihn unter folgendem URL:

Online-Registrierungssystem

Den Wartungsvertrag verlängern

Trend Micro oder dazu autorisierte Händler bieten allen registrierten Benutzern technischen Support, Downloads und Programm-Updates für die Dauer eines (1) Jahres. Nach Ablauf dieser Frist muss der Wartungsvertrag verlängert werden.

Nach Ablauf des Wartungsvertrags sind grundlegende Operationen weiter verfügbar. Sie können jedoch keine neuen Benutzer und Geräte zu PolicyServer hinzufügen, weder über PolicyServer MMC, über Agent-Installationen noch über Control Manager. Daher sollte der Wartungsvertrag sobald wie möglich verlängert werden.

Wenn Kunden ein Upgrade durchführen, wird die vorhandene Lizenz bis zum Ablauf akzeptiert.

Prozedur

1. Gehen Sie wie folgt vor, um den Wartungsvertrag zu verlängern:

   - Wenden Sie sich an den Händler, bei dem Sie auch das Produkt erworben haben. Die Verlängerung des Wartungsvertrags um ein weiteres Jahr wird per Post an den Hauptansprechpartner für Registrierungsfragen gesendet.

   - Melden Sie sich auf der Trend Micro Website für die Online-Registrierung an, um die Registrierungsdaten Ihres Unternehmens anzuzeigen oder zu ändern: https://olr.trendmicro.com/registration/

2. Um die Registrierungsdaten anzuzeigen, geben Sie die Anmelde-ID und das Kennwort an, die Sie bei der ersten Registrierung des Produkts bei Trend Micro (als Neukunde) erstellt haben, und klicken Sie anschließend auf **Anmelden**.

3. Informationen zur Aktualisierung der Umgebung mit dem neuen Aktivierungscode finden Sie unter *Neue Produktlizenz aktivieren auf Seite 8-3*.

Testlizenz

Sie können Endpoint Encryption für einen zeitlich begrenzten Testzeitraum von 30 Tagen installieren und bewerten. Während der Installation von PolicyServer werden die Unternehmensdatenbank und das Unternehmensadministratorkonto angelegt. PolicyServer funktioniert normal mit allen Client-Anwendungen, einer unbegrenzten Zahl von Geräten und bis zu 100 Benutzern für einen Testzeitraum von 30 Tagen. Wenden Sie sich nach 30 Tagen an den Technischen Support von Trend Micro, um eine Lizenzdatei zu erhalten. Nach Ablauf des Testzeitraums funktionieren Endpoint Encryption Benutzerkonten und Geräte normal.

Neue Produktlizenz aktivieren

Eine kostenfreie Testlizenz für 30 Tage ist verfügbar, um Endpoint Encryption zu installieren und zu bewerten. Wenn Sie von der Testlizenz aus auf eine Produktlizenz umsteigen, stellen Sie sicher, dass Sie vor Ablauf der Lizenz das Upgrade auf die Vollversion durchführen.

Prozedur

1. Melden Sie sich bei dem Server an, auf dem PolicyServer momentan installiert ist.
2. Navigieren Sie zu dem Ordner, der die Programmdateien von PolicyServer enthält, und öffnen Sie den Ordner `Tools`.
3. Führen Sie `TMEE_License_Renewal.exe` aus.

   Das **Tool zur Lizenzverlängerung** wird geöffnet.
4. Klicken Sie unter **Lizenz verlängern** auf **Online verlängern**, um auf die Registrierungs-Website von Trend Micro zuzugreifen.

   Nach Abschluss der Registrierung erhalten Sie von Trend Micro eine E-Mail mit dem Aktivierungscode.
5. Geben Sie den neuen Aktivierungscode für das Produkt ein.
6. Klicken Sie auf **Aktivieren**.
7. Wenn die Bestätigungsmeldung angezeigt wird, klicken Sie auf **OK**, um fortzufahren.
8. Klicken Sie auf **Beenden**.

Die aktualisierte Endpoint Encryption Produktlizenz ist sofort verfügbar.

Produktlizenz anzeigen

Sie können mit PolicyServer MMC den aktuellen Status der Lizenz anzeigen.

Prozedur

1. Melden Sie sich bei PolicyServer MMC an.
2. Klicken Sie mit der rechten Maustaste auf das Unternehmen, und wählen Sie **Aktivierung/Lizenz**.

   Das Fenster **Registrierungsinformationen** wird angezeigt.
3. Überprüfen Sie die folgenden Optionen.

OPTION	BEZEICHNUNG
Aktivierungscode	Bei einer Vollversion wird der Aktivierungscode angezeigt. Bei anderen Lizenztypen wird der Name der Lizenz angezeigt.
Anfangsdatum	Das Datum, an dem die Lizenz aktiviert wurde.
Ablaufdatum	Das Datum, an dem die Lizenz verlängert werden muss. Nach dem Ablauf einer Lizenz können vorhandene Endpoint Encryption Benutzer sich weiterhin bei Endpoint Encryption Geräten anmelden, jedoch können keine neuen Endpoint Encryption Geräte oder Benutzer dem Unternehmen hinzugefügt werden.
Anzahl der Geräte	Die laut der Lizenz zulässige Anzahl der Endpoint Encryption Geräte.
Anzahl der installierten Geräte	Die im Unternehmen momentan konfigurierte Anzahl der Endpoint Encryption Geräte.
Anzahl der Benutzer	Die laut der Lizenz zulässige Gesamtzahl der Endpoint Encryption Benutzer.
Anzahl der erstellten Benutzer	Die dem Unternehmen momentan hinzugefügte Anzahl an Endpoint Encryption Benutzern.
Aktivierungszeitraum in Tagen	Die Anzahl der verbleibenden Tage bis zum Ablauf der Lizenz.

4. Klicken Sie auf **Schließen**.

Produktwartung

Von Zeit zu Zeit wird Trend Micro möglicherweise einen Patch für ein gemeldetes bekanntes Problem oder ein Upgrade für das Produkt veröffentlichen. Wenn Sie herausfinden möchten, ob Patches verfügbar sind, besuchen Sie: http://downloadcenter.trendmicro.com/?regs=DE

Patches sind mit einem Datum versehen. Falls Patches vorliegen, öffnen Sie die Readme-Datei, um festzustellen, ob der Patch anwendbar ist. Falls ja, befolgen Sie die Upgrade-Anweisungen in der Readme-Datei.

Ressourcen zur Fehlerbehebung

Bevor Sie mit dem technischen Support Kontakt aufnehmen, sollten Sie die folgenden Online-Ressourcen von Trend Micro besuchen:

Trend Community

Um Hilfe zu erhalten, Erfahrungen auszutauschen, Fragen zu stellen und Sicherheitsprobleme mit anderen Benutzern, Enthusiasten und Sicherheitsexperten zu diskutieren, navigieren Sie zu:

http://community.trendmicro.com/

Das Support-Portal verwenden

Beim Trend Micro Support Portal handelt es sich um eine Online-Ressource mit brandaktuellen Informationen über häufige und ungewöhnliche Probleme, auf die Sie rund um die Uhr zugreifen können.

Prozedur

1. Gehen Sie zu http://esupport.trendmicro.com.
2. Wählen Sie ein Produkt oder einen Dienst aus dem entsprechenden Listenfeld aus, und geben Sie weitere verwandte Informationen an, wenn Sie dazu aufgefordert werden.

   Die Produktseite **Technischer Support** wird angezeigt.
3. Suchen Sie über das Feld **Support durchsuchen** nach verfügbaren Lösungen.

4. Wenn keine Lösung gefunden wird, klicken Sie in der linken Navigationsleiste auf **Submit a Support Case**, und fügen Sie relevante Details hinzu, oder übermitteln Sie den Support-Fall hier:

   http://esupport.trendmicro.com/srf/SRFMain.aspx

   Ein Trend Micro Support-Ingenieur untersucht den Fall und antwortet innerhalb von 24 Stunden oder schneller.

Security Intelligence Community

Die Cybersecurity-Experten von Trend Micro sind ein Eliteteam im Bereich Security Intelligence, das sich auf Erkennung und Analyse von Bedrohungen, Sicherheit in Cloud- und virtualisierten Umgebungen sowie Datenverschlüsselung spezialisiert hat.

Navigieren Sie zu http://www.trendmicro.de/sicherheitsinformationen/index.html. Sie finden dort Informationen über:

- Trend Micro Blogs, Twitter, Facebook, YouTube und andere soziale Medien
- Bedrohungsberichte, Forschungsarbeiten und Spotlight-Artikel
- Lösungen, Podcasts und Newsletter von globalen Insidern aus der Sicherheitsbranche
- Kostenlose Tools, Apps und Widgets.

Bedrohungsenzyklopädie

Die meiste Malware besteht aus "kombinierten Bedrohungen", d. h., mindestens zwei Technologien wurden kombiniert, um die Sicherheitsprotokolle des Computers zu umgehen. Trend Micro bekämpft diese komplexe Malware mit Produkten, die eine benutzerdefinierte Verteidigungsstrategie schaffen. Die Bedrohungsenzyklopädie stellt eine umfangreiche Liste aus Namen und Symptomen für verschiedene kombinierte Bedrohungen bereit, einschließlich bekannter Malware, Spam, bösartiger URLs und bekannter Schwachstellen.

Navigieren Sie zu http://www.trendmicro.com/vinfo/de/virusencyclo/default.asp. Sie finden dort weitere Informationen über:

- Malware und bösartige mobile Codes, die zum jeweiligen Zeitpunkt aktiv oder im Umlauf sind
- Zusammenhängende Seite mit Bedrohungsinformationen, die ein vollständiges Bild der Webangriffe zeichnen
- Beratung zu Internet-Bedrohungen über gezielte Angriffe und Sicherheitsbedrohungen
- Informationen zu Webangriffen und Online-Trends
- Wöchentliche Malware-Berichte.

Kontaktaufnahme mit Trend Micro

Trend Micro Mitarbeiter sind per Telefon, Fax oder E-Mail verfügbar:

Adresse	Trend Micro Deutschland GmbH Zeppelinstraße 1 Hallbergmoos, Bayern 85399 Deutschland
Tel.	+49 (0) 811 88990-700
Fax	+4981188990799
Internet-Adresse	http://www.trendmicro.de/
E-Mail	support@trendmicro.com

- Weltweite Support-Büros:

  http://www.trendmicro.de/ueber-uns/kontakt/index.html

- Trend Micro Produktdokumentation:

  http://docs.trendmicro.com/de-de/home.aspx

Problemlösung beschleunigen

Um das Lösen eines Problems zu verbessern, halten Sie die folgenden Informationen bereit:

- Schritte, um das Problem nachvollziehen zu können
- Informationen zu Gerät oder Netzwerk
- Marke und Modell des Computers sowie weitere, an den Endpunkt angeschlossene Hardware
- Größe des Arbeitsspeichers und des freien Festplattenspeichers
- Version und Service Pack des verwendeten Betriebssystems
- Endpunkt-Clientversion
- Seriennummer oder Aktivierungscode
- Ausführliche Beschreibung der Installationsumgebung
- Genauer Wortlaut eventueller Fehlermeldungen

Andere Ressourcen

Neben den Lösungen und dem Support sind online viele andere hilfreiche Ressourcen verfügbar, die Ihnen helfen, auf dem Laufenden zu bleiben, über Innovationen informiert zu werden und Informationen über aktuelle Sicherheitsbedrohungen zu erhalten.

TrendEdge

Sie können nach Informationen über nicht unterstützte, innovative Techniken, Tools und bewährte Methoden für Produkte und Dienste von Trend Micro suchen. Die TrendEdge Datenbank enthält zahlreiche Dokumente zu vielen verschiedenen Themen für Partner, Mitarbeiter oder andere interessierte Parteien von Trend Micro.

Die neuesten Informationen, die in TrendEdge aufgenommen wurden, finden Sie unter:

http://trendedge.trendmicro.com/

Download Center

Von Zeit zu Zeit wird Trend Micro möglicherweise einen Patch für ein gemeldetes bekanntes Problem oder ein Upgrade für ein bestimmtes Produkt oder einen bestimmten Dienst veröffentlichen. Wenn Sie herausfinden möchten, ob Patches verfügbar sind, besuchen Sie:

http://downloadcenter.trendmicro.com/?regs=DE

Wenn ein Patch noch nicht angewendet wurde (Patches sind mit Datumsangaben versehen), öffnen Sie die Readme-Datei, um festzustellen, ob der Patch für Ihre Umgebung von Bedeutung ist. In der Readme-Datei finden Sie auch die Installationsanweisungen.

TrendLabs

TrendLabs℠ ist ein weltweites Netzwerk aus Forschungs-, Entwicklungs- und Lösungszentren, das rund um die Uhr Bedrohungen überwacht, Präventionsstrategien entwickelt sowie rasche und kontinuierliche Lösungen bereitstellt. TrendLabs bildet die Grundlage der Trend Micro Service-Infrastruktur und beschäftigt mehrere hundert Mitarbeiter und zertifizierte Support-Experten, die sich um die vielfältigen Anfragen zu Produkten und technischem Support kümmern.

TrendLabs überwacht die weltweite Bedrohungslage und liefert wirksame Sicherheitsmaßnahmen für die Erkennung, Vermeidung und Beseitigung von Angriffen. Die Kunden profitieren von diesen täglichen Bemühungen in Form von häufigen Viren-Pattern-Updates und Erweiterungen der Scan Engine.

Weitere Informationen über TrendLabs finden Sie unter:

http://www.trendmicro.de/newsroom/faces/index.html

Anhänge

Anhänge



Anhang A

Einführung in Trend Micro™ Control Manager™

Der Trend Micro Control Manager ist eine zentrale Management-Konsole zur Verwaltung von Produkten und Services von Trend Micro auf Gateways, Mail-Servern, File-Servern und Unternehmensdesktops. Administratoren können mit den Funktionen zur Richtlinienverwaltung die Produkteinstellungen für die verwalteten Produkte und Endpunkte konfigurieren und verteilen. Die webbasierte Management-Konsole von Control Manager bietet einen zentralen Überwachungspunkt für die Verwaltung der Produkte und Dienste für Virenschutz und Content Security im gesamten Netzwerk.

Mit Control Manager kann der Systemadministrator Aktivitäten wie beispielsweise auftretende Virenausbrüche, Sicherheitsverstöße oder mögliche Viren-/Malware-Eintrittsstellen überwachen und aufzeichnen. Der Systemadministrator kann Update-Komponenten herunterladen und im Netzwerk verteilen und somit einen einheitlichen und aktuellen Schutz gewährleisten. Zu den Beispielen für Update-Komponenten zählen die Viren-Pattern-Dateien, die Scan Engine und die Anti-Spam-Regeln. Mit Control Manager sind sowohl manuelle als auch zeitgesteuerte Updates möglich. Mit Control Manager können Produkte in Gruppen oder einzeln konfiguriert und verwaltet werden.

Dieses Kapitel umfasst die folgenden Themen:

Control Manager Standard und Advanced

Control Manager ist in zwei Versionen erhältlich: Standard und Advanced. Control Manager Advanced enthält Funktionen, die in Control Manager Standard nicht enthalten sind. Beispielsweise unterstützt Control Manager Advanced eine übersichtlich gegliederte Verwaltungsstruktur. Das bedeutet, das Control Manager Netzwerk kann von einem übergeordneten Control Manager Advanced Server verwaltet werden, wobei mehrere untergeordnete Control Manager Advanced Server Meldungen an den übergeordneten Control Manager Advanced Server senden. Der übergeordnete Server erfüllt die Aufgaben eines Knotenpunkts für das gesamte Netzwerk.



Hinweis

Control Manager Advanced unterstützt die folgenden untergeordneten Control Manager Server:

- Control Manager 6.0 Advanced
- Control Manager 5.5 Advanced
- Control Manager 5.0 Advanced

Control Manager 5.0/5.5/6.0 Standard Server werden als untergeordnete Server nicht unterstützt.

Eine vollständige Liste aller Funktionen der Standard- und Advanced-Versionen von Control Manager Server finden Sie in der *Trend Micro Control Manager* Dokumentation.

Einführung in die Funktionen von Control Manager

Control Manager wurde von Trend Micro zur Verwaltung von Antiviren- und Content-Security-Produkten und Diensten entwickelt, die in den LANs und WANs eines Unternehmens eingesetzt werden.

TABELLE A-1. Control Manager Funktionen

FUNKTION	BESCHREIBUNG
Richtlinienverwaltung	Systemadministratoren können von einer einzelnen Management-Konsole aus mit Hilfe von Richtlinien Produkteinstellungen für verwaltete Produkte und Endpunkte konfigurieren und verteilen.
Zentrale Konfiguration	Mit dem Produktverzeichnis und einer übersichtlich gegliederten Verwaltungsstruktur können Sie mit Hilfe dieser Funktionen Reaktionen auf Viren und Content-Security-Aufgaben von einer einzelnen Management-Konsole aus koordinieren. Diese Funktionen tragen dazu bei, die einheitliche Durchsetzung der Viren/Malware- und Content-Security-Richtlinien in Ihrem Unternehmen sicherzustellen.
Proaktive Ausbruchsprävention	Mit den Outbreak Prevention Services (OPS) schützen Sie Ihr Netzwerk proaktiv vor einem bevorstehenden Viren-/ Malware-Ausbruch.
Sichere Kommunikationsinfrastrukt ur	Die Kommunuikationsinfrastruktur des Control Managers basiert auf dem Secure Socket Layer (SSL) Protokoll. Je nach gewählter Sicherheitseinstellung kann der Control Manager Nachrichten mit oder ohne Authentifizierung verschlüsseln.
Sichere Konfiguration und sicherer Komponenten-Download	Mit diesen Funktionen können Sie einen sicheren Zugriff auf die Webkonsole und einen sicheren Komponenten-Download konfigurieren.
Aufgabenverteilung	Der Systemadministrator kann den Benutzern der Webkonsole von Control Manager personalisierte Konten mit benutzerdefinierten Berechtigungen einrichten. In den Benutzerkonten ist festgelegt, was der Benutzer in einem Control Manager Netzwerk sehen und welche Aktionen er durchführen kann. Die Nutzung der Konten kann über Benutzerprotokolle nachverfolgt werden.

FUNKTION	BESCHREIBUNG
Befehlsverfolgung	Mit dieser Funktion können Sie alle Befehle überwachen, die auf der Webkonsole von Control Manager ausgeführt werden. Das Rückverfolgen von Befehlen ist eine nützliche Option zur Überprüfung, ob Control Manager lang andauernde Befehle erfolgreich ausgeführt hat, wie z. B. das Update und die Verteilung von Viren-Pattern.
Manuelle Produktsteuerung	Verwaltete Produkte in Echtzeit steuern. Control Manager sendet Konfigurationsänderungen, die über die Webkonsole durchgeführt wurden, umgehend an die verwalteten Produkte. Systemadministratoren können manuelle Suchen über die Webkonsole ausführen. Dieses Befehlssystem ist bei einem Viren-/Malware-Ausbruch unverzichtbar.
Zentrale Update-Steuerung	Aktualisiert Viren-Pattern, Anti-Spam-Regeln, Scan Engines und andere Antiviren- oder Content-Security-Komponenten, die dazu beitragen, dass alle verwalteten Produkte aktuell sind.
Zentrale Berichterstellung	Gibt einen Überblick über die Leistung der Antiviren- und Content-Security-Produkte mit Hilfe von umfangreichen Protokollen und Berichten. Control Manager erfasst die Protokolle von allen verwalteten Produkten, d. h., Sie müssen nicht mehr die Protokolle der jeweiligen einzelnen Produkte überprüfen.

Control Manager Architektur

Trend Micro Control Manager bietet Funktionen, um Produkte und Dienste von Trend Micro von einer zentralen Stelle aus zu steuern. Diese Anwendung vereinfacht die Verwaltung der Viren/Malware- und Content-Sicherheitsrichtlinien im Unternehmen. Die folgende Tabelle enthält eine Liste der Komponenten, die von Control Manager verwendet werden.

TABELLE A-2. Control Manager Komponenten

KOMPONENTE	BESCHREIBUNG
Control Manager server	Dient als ein Repository für alle Daten, die von den Agents erfasst werden. Dabei kann es sich um Server der Standard Edition oder der Advanced Edition handeln. Ein Control Manager Server unterstützt die folgenden Funktionen: • Eine SQL-Datenbank, in der die Konfigurationen und die Protokolle der verwalteten Produkte gespeichert werden. Control Manager arbeitet mit der Datenbank Microsoft SQL Server (`db_ControlManager.mdf`) zusammen, um Daten zu speichern, die in Protokollen, Communicator Zeitplänen, verwalteten Produkten und Informationen zu untergeordneten Servern, Benutzerkonten, Netzwerkumgebungen und Benachrichtigungseinstellungen enthalten sind. • Ein Webserver als Host für die Webkonsole von Control Manager. • Ein Mail-Server, der die Benachrichtigungen bei Ereignissen in Form von E-Mail-Nachrichten versendet. Control Manager kann Benachrichtigungen an Einzelpersonen oder Empfängergruppen über Ereignisse senden, die im Control Manager Netzwerk auftreten. In Event Center können Sie konfigurieren, ob Benachrichtigungen als E-Mail-Nachrichten, Windows Ereignisprotokoll, MSN Messenger, SNMP, Syslog, Pager oder an eine andere interne oder dem Branchenstandard entsprechende Anwendung gesendet werden, die von Ihrem Unternehmen zur Versendung von Benachrichtigungen eingesetzt wird. • Ein Berichtserver, der nur zum Umfang der Advanced Edition gehört, generiert Berichte zu Antiviren- und Content-Sicherheitsprodukten. Ein Control Manager Bericht ist eine Online-Sammlung von Zahlen über das Auftreten von Ereignissen zu Sicherheitsbedrohungen und Content-Sicherheit im Control Manager Netzwerk, die ein Sicherheitsrisiko darstellen.

Komponente	Beschreibung
Das Trend Micro Management Communication Protocol	MCP verarbeitet die Interaktion von Control Manager Server mit den verwalteten Produkten, die den Agent der nächsten Generation unterstützen. MCP ist das neue Rückgrat für das Control Manager System. MCP Agents werden mit den verwalteten Produkten installiert und nutzen eine Ein-Weg- oder Zwei-Wege-Kommunikation zur Kommunikation mit Control Manager. MCP Agents rufen Anweisungen und Updates vom Control Manager ab.
Trend Micro Management Infrastructure	Verarbeitet die Interaktion von Control Manager Server mit älteren verwalteten Produkten. Der Communicator bzw. das Message Routing Framework ist das Kommunikationsrückgrat für das ältere Control Manager System. Dabei handelt es sich um eine Komponente der Trend Micro Management Infrastructure (TMI). Communicators verarbeiten die gesamte Kommunikation zwischen dem Control Manager Server und den älteren verwalteten Produkten. Die Kommunikation mit den älteren verwalteten Produkten erfolgt durch Interaktion mit Control Manager 2.x Agents.
Control Manager 2.x Agents	Empfangen Befehle von Control Manager Server und senden Statusinformationen und Protokolle an den Control Manager Server Beim Control Manager Agent handelt es sich um eine Anwendung, die auf dem Server eines verwalteten Produkts installiert ist und die es möglich macht, dass Control Manager das Produkt verwaltet. Agents interagieren mit dem verwalteten Produkt und Communicator. Ein Agent dient als Brücke zwischen dem verwalteten Produkt und Communicator. Aus diesem Grund sollten Sie alle Agents auf demselben Computer wie die verwalteten Produkte installieren.

KOMPONENTE	BESCHREIBUNG
Webbasierte Management-Konsole	Ermöglicht, dass ein Administrator Control Manager von quasi jedem Computer mit einer Internet-Verbindung und Windows™ Internet Explorer™ aus verwaltet. Bei der Management-Konsole von Control Manager handelt es sich um eine Web-basierte Konsole, die im Internet über den Microsoft Internet Information Server (IIS) veröffentlicht wurde und die vom Control Manager Server gehostet wird. Mit dieser Lösung können Sie das Control Manager Netzwerk von einem beliebigen Computer verwalten, auf dem ein kompatibler Webbrowser verwendet wird.
Widget-Framework	Ermöglicht Administratoren, ein angepasstes Dashboard zur Überwachung des Control Manager Netzwerks zu erstellen.

Endpoint Encryption bei Control Manager registrieren

Sie können den Endpoint Encryption Server erst bei einem Control Manager Server registrieren, nachdem Sie sichergestellt haben, dass der Server und der Control Manager Server zum selben Netzwerksegment gehören.

Prozedur

1. Klicken Sie auf **Administration** > **Control Manager Settings**.

   Hinweis

   Control Manager verwendet den Namen, den Sie im Feld "Host-Name" angegeben haben, um den Endpoint Encryption Server zu identifizieren. Der Host-Name wird im Produktverzeichnis von Control Manager angezeigt.

   Das Fenster **Control Manager Settings** wird angezeigt.

2. Geben Sie unter **Connection settings** den Namen des Endpoint Encryption Servers in das Feld **Entity display name** ein.

3. Legen Sie unter **Control Manager Server Settings** die folgenden Einstellungen fest:

    a. Geben Sie den Host-Namen oder die IP-Adresse des Control Manager Servers in das Eingabefeld "Server-FQDN" oder "IP-Adresse" ein.

    b. Geben Sie die Portnummer des MCP Agents ein, der für die Kommunikation mit Control Manager verantwortlich ist.

    c. Wenn Sie für die Sicherheit von Control Manager "Mittel" festgelegt haben (Kommunikation über HTTPS und HTTP ist zulässig zwischen Control Manager und dem MCP Agent der verwalteten Produkte), wählen Sie **Connect through HTTPS**.

    d. Wenn Ihr Netzwerk eine Authentifizierung erfordert, geben Sie den Benutzernamen und das Kennwort des IIS-Servers in die Felder **Username** und **Password** ein.

    e. Wenn Sie ein NAT-Gerät einsetzen, wählen Sie **Enable two-way communication port forwarding**, und geben Sie die IP-Adresse und Portnummer des NAT-Geräts in die Felder **IP address** und **port number** ein.

    Weitere Informationen zur Verwaltung von Produkten in Control Manager finden Sie im *Administratorhandbuch für Trend Micro Control Manager*.

4. Klicken Sie auf der Management-Konsole von Control Manager auf **Products**.

    Das Fenster **Product Directory** wird angezeigt.

5. Der Endpoint Encryption Server wird im Produktverzeichnis angezeigt.

Grundlegendes zum Benutzerzugriff

Die Zugriffskontrolle von Control Manager besteht aus den folgenden vier Abschnitten.

TABELLE A-3. Optionen für den Control Manager Benutzerzugriff

ABSCHNITT	BESCHREIBUNG
Mein Konto	Das Fenster **My Account** enthält die Kontodaten, über die Control Manager für einen bestimmten Benutzer verfügt. Die Informationen im Fenster **My Account** sind vom Benutzer abhängig.
Benutzerkonten	Im Fenster **User Accounts** werden alle Benutzer von Control Manager angezeigt. Das Fenster enthält ebenfalls Optionen für Benutzer, die Control Manager Benutzerkonten erstellen und pflegen möchten. Mit Hilfe dieser Funktionen definieren Sie klare Verantwortungsbereiche für Benutzer, indem Sie die Zugriffsrechte auf bestimmte verwaltete Produkte einschränken und begrenzen, welche Aktionen Benutzer auf den verwalteten Produkten ausführen können. Diese Funktionen sind: • Ausführen • Konfigurieren • Verzeichnis bearbeiten
Benutzerrollen	Im Fenster **User Roles** werden alle Benutzerrollen von Control Manager angezeigt. Das Fenster enthält ebenfalls Optionen für Benutzer, die Control Manager Benutzerrollen erstellen und pflegen möchten. Mit Benutzerrollen wird definiert, auf welche Bereiche der Webkonsole von Control Manager ein Benutzer Zugriff hat.

ABSCHNITT	BESCHREIBUNG
Benutzergruppen	Im Fenster **User Groups** befinden sich die Control Manager Gruppen sowie Optionen zum Erstellen von Gruppen. Control Manager verwendet Gruppen als einfache Methode, um Benachrichtigungen an mehrere Benutzer zu senden, ohne dass dazu die Benutzer einzeln ausgewählt werden müssten. Control Manager lässt es nicht zu, dass Administratoren eine Gruppe mit denselben Zugriffsrechten wie eine andere Gruppe erstellen.



Hinweis

Sie können Benutzern verschiedene Zugriffsrechte und Berechtigungen zuweisen, um bestimmte Verwaltungsaufgaben zu delegieren, ohne dazu die Sicherheit zu beeinträchtigen.

Control Manager Benutzerzugriff mit Endpoint Encryption Benutzerzugriff

Der Benutzerzugriff von Endpoint Encryption entspricht dem Benutzerzugriff von Control Manager. Administratoren können festlegen, auf welche Teile der Webkonsole von Endpoint Encryption der Benutzer Zugriff hat (Power-User, Bediener oder Administrator).

Alle Benutzerkonten, die in Control Manager erstellt wurden, haben Administratorzugriff auf alle verwalteten Produkte, auf die der Benutzer Zugriff hat. Daraus ergibt sich ein Problem, wenn ein Administrator den Benutzerzugriff auf dem Endpoint Encryption System auf "Power User" reduzieren will, während der Zugriff auf Control Manager zugelassen wird.

MCP-Rückmeldung

Um den Status der verwalteten Produkte zu überwachen, fragen MCP Agents den Control Manager auf Grundlage eines Zeitplans ab. Dadurch kann der Status des

verwalteten Produkts angezeigt und überprüft werden, ob Befehle von Control Manager an das verwaltete Produkt vorliegen. Die Webkonsole von Control Manager zeigt dann den Produktstatus an. Dies bedeutet, dass der Status des verwalteten Produkts nicht in Echtzeit dargestellt wird. Control Manager überprüft sequenziell im Hintergrund den Status eines jeden verwalteten Produkts. Control Manager ändert den Status der verwalteten Produkte in Offline, wenn das verwaltete Produkt sich innerhalb eines festgelegten Zeitraums nicht zurückmeldet.

Control Manager kann den Status der verwalteten Produkte nicht nur durch aktive Rückmeldungen feststellen. Auch die folgenden Funktionen liefern Control Manager Informationen über den Status des verwalteten Produkts:

- Control Manager erhält Protokolle vom verwalteten Produkt. Wenn Control Manager erfolgreich ein Protokoll vom verwalteten Produkt empfängt, wird davon ausgegangen, dass das verwaltete Produkt ordnungsgemäß funktioniert.
- Im Zwei-Wege-Kommunikationsmodus versendet Control Manager aktiv eine Benachrichtigung an das verwaltete Produkt, damit dieses den anstehenden Befehl abruft. Wenn der Server erfolgreich eine Verbindung zum verwalteten Produkt herstellt, ist auch dies ein Anzeichen dafür, dass das Produkt ordnungsgemäß funktioniert, und dieses Ereignis zählt als Rückmeldung.
- Im Ein-Wege-Kommunikationsmodus sendet der MCP Agent periodisch Abfragebefehle an Control Manager. Dieses Verhalten entspricht einer Rückmeldung und wird von Control Manager als solche behandelt.

Die MCP-Rückmeldungen können in verschiedener Weise erfolgen:

- **UDP**: Die einfachste und schnellste Lösung ist eine Verbindung zwischen dem Produkt und dem Server über UDP. In NAT- oder Firewall-Umgebungen ist diese Lösung nicht möglich. Der Client, der die Anfrage überträgt, kann jedoch nicht überprüfen, ob der Server die Anfrage erhält.
- **HTTP/HTTPS**: In einer NAT- oder Firewall-Umgebung erfolgt die Rückmeldung über eine schwerfälligere HTTP-Verbindung.

Control Manager unterstützt die Übertragung von Rückmeldungen über UDP und HTTP/HTTPS. Control Manager Server stellt fest, welchen Modus das verwaltete Produkt während des Registrierungsvorgangs anwendet. Der Modus wird durch einen separaten Protokoll-Handshake zwischen beiden Parteien festgelegt.

Neben der Rückmeldung des Produktstatus können zusätzliche Daten an Control Manager gesendet werden. Diese Daten enthalten üblicherweise Informationen über die Aktivität des verwalteten Produkts, die auf der Konsole angezeigt werden.

Die Zeitplanleiste verwenden

Mit Hilfe der Zeitplanleiste im Fenster **Agent Communication Schedule** können Sie Communicator-Zeitpläne anzeigen und bearbeiten. Die Leiste hat 24 Positionen, von denen jede eine Stunde des Tages darstellt.

Die Felder mit den Uhrsymbolen zeigen den Arbeitsstatus bzw. die Stunden an, an dem bzw. zu denen der Agent/Communicator Informationen an den Control Manager Server senden soll. Weiße Positionen zeigen die Ruhezeit an. Definieren Sie Arbeits- oder Ruhezeiten durch die Auswahl bestimmter Positionen.

Sie können höchstens drei aufeinander folgende inaktive Zeiträume angeben. Die Schedule Bar im Beispiel unten zeigt nur zwei inaktive Zeiträume:

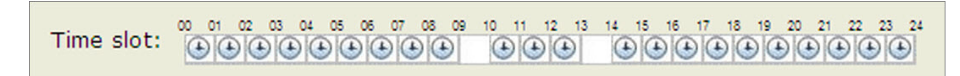


ABBILDUNG A-1. Zeitplanleiste

Die in der Leiste angegebenen aktiven Zeiträume sind 0:00 bis 7:00, 8:00 bis 16:00 und von 18:00 bis 24:00.

Einen Zeitplan für die Kommunikation mit Agents für ein verwaltetes Produkt festlegen

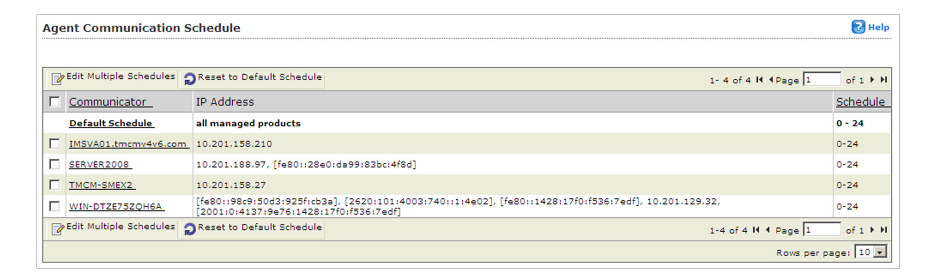
---

Prozedur

1. Öffnen Sie die Control Manager Konsole.

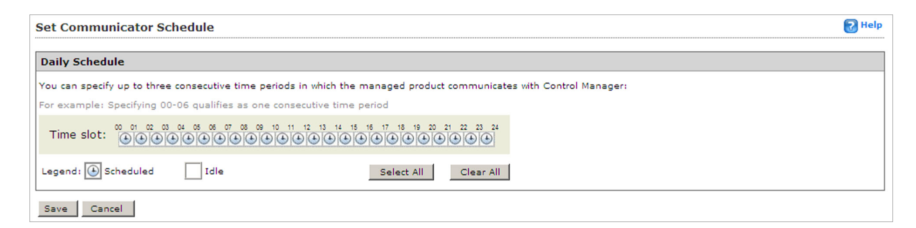
2. Navigieren Sie zu **Administration** > **Settings** > **Agent Communication Schedule**.

   Das Fenster **Agent Communication Schedule** wird angezeigt.



3. Wählen Sie den Zeitplan für das verwaltete Produkt, der geändert werden soll.

   Das Fenster **Set Communicator Schedule** wird angezeigt.



4. Definieren Sie den Zeitplan. Geben Sie eine neue Uhrzeit an, oder verwenden Sie die Standardeinstellung:

   - Zum Angeben einer neuen Einstellung ändern Sie die entsprechenden Zeitpositionen in der Zeitplanleiste, und klicken Sie anschließend auf **Save**
   - Wenn Sie die Standardeinstellung verwenden möchten, kehren Sie zum Fenster **Agent Communication Schedule** zurück. Wählen Sie den Zeitplan, der angewendet werden soll, und klicken Sie auf **Reset to Default Schedule**

Die richtige Einstellung für Rückmeldungen ermitteln

Bei der Einstellung der Rückmeldungen ist zu berücksichtigen, dass einerseits die neuesten Statusinformationen des verwalteten Produkts angezeigt, andererseits aber auch die Systemressourcen effizient gehandhabt werden müssen. Die Standardeinstellung bringt in den meisten Fällen zufriedenstellende Ergebnisse, Sie sollten jedoch die folgenden Punkte berücksichtigen, wenn Sie die Einstellung für die Rückmeldung anpassen:

TABELLE A-4. Empfehlungen für Rückmeldungen

ZEITINTERVALL FÜR RÜCKMELDUNGEN	EMPFEHLUNG
Lange Intervalle zwischen Rückmeldungen (mehr als 60 Minuten)	Je länger das Intervall zwischen den Rückmeldungen ist, desto größer ist die Anzahl der Ereignisse, die eintreten können, bevor Control Manager den Communicator-Status auf der Web-Konsole anzeigt. Wird z. B. ein Verbindungsproblem mit einem Communicator zwischen zwei Rückmeldungen gelöst, so kann eine Kommunikation mit einem Communicator stattfinden, selbst wenn der Status als (inaktiv) oder (unnormal) angezeigt wird.
Kurze Intervalle zwischen Rückmeldungen (weniger als 60 Minuten)	Bei kurzen Intervallen zwischen den Rückmeldungen ergibt sich auf dem Control Manger Server ein aktuelleres Bild Ihres Netzwerkstatus. Diese Option erfordert allerdings eine hohe Bandbreite.

Rückmeldung von Agent Communicator konfigurieren

Im Fenster **Communication Time-out** definieren Sie die Frequenz und die maximalen Verzögerungszeiten (in Minuten) für den Control Manager Server und die Agent-Kommunikation.



Hinweis

Die Einstellung für die Rückmeldung von Agent/Communicator gilt nur für Communicators für verwaltete Produkte, die direkt vom Control Manager Server gesteuert werden. Untergeordnete Agents/Communicators für Control Manager Server verwenden vordefinierte Werte:

Frequency: 3 Minuten

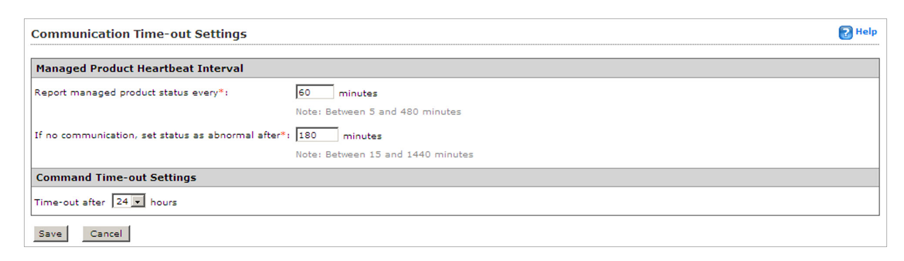
Maximum delay: 5 Minuten

Prozedur

1. Öffnen Sie die Control Manager Konsole.

2. Navigieren Sie zu **Administration** > **Settings** > **Communication Time-out Settings**.

   Das Fenster **Communication Time-out** wird angezeigt.



3. Im Arbeitsbereich können Sie entweder die Standardwerte belassen oder neue Einstellungen für Folgendes festlegen:

   - **Report managed product status every**: Definiert, wie oft das verwaltete Produkt auf Meldungen vom Control Manager Server reagiert. Gültige Werte liegen zwischen 5 und 480 Minuten

   - **If no communication, set status as abnormal after**: Gibt an, wie lange Control Manager auf eine Antwort vom verwalteten Produkt wartet, bevor der Status der Webkonsole auf (inaktiv) geändert wird. Gültige Werte liegen zwischen 15 und 1440 Minuten.



Hinweis

Der Wert für **If no communication, set status as abnormal after** muss wenigstens dreimal so hoch sein wie der Wert für **Report managed product status every**.

4. Klicken Sie auf **Save**.

Grundlegendes zum Produktverzeichnis

Bei einem verwalteten Produkt handelt es sich um eine Repräsentation eines Antivirus-, Content-Sicherheit- oder Web-Schutz-Produkts im Produktverzeichnis. Verwaltete Produkte werden als Symbole (Beispiel: (SMEX) oder (FW)) auf der Webkonsole von Control Manager, Abschnitt Produktverzeichnis, angezeigt. Diese Symbole stellen die Produkte von Trend Micro zu Antivirus, Content-Sicherheit und Schutz vor Internet-Bedrohungen dar. Control Manager unterstützt dynamische Symbole, die sich je nach Status des verwalteten Produkts ändern. Weitere Informationen zu den Symbolen und den damit in Zusammenhang stehenden Statuszuständen des verwalteten Produkts finden Sie in der Dokumentation zum betreffenden verwalteten Produkt.

Sie können verwaltete Produkte entweder individuell oder indirekt mit Hilfe von Gruppen über das Produktverzeichnis verwalten. In der folgenden Tabelle werden die Menübefehle und Schaltflächen im Fenster "Produktverzeichnis" aufgeführt.

Tabelle A-5. Optionen des Produktverzeichnisses

Menüelement	Beschreibung
Erweiterte Suche	Klicken Sie auf diesen Menübefehl, um die Suchkriterien für eine Suche nach einem oder mehreren verwalteten Produkten anzugeben.
Konfigurieren	Bewegen Sie nach der Auswahl eines verwalteten Produkts/Verzeichnisses den Mauszeiger über diesen Menübefehl, und wählen Sie eine Aufgabe aus, um sich bei einer Web-basierte Konsole mit SSO anzumelden oder ein verwaltetes Produkt zu konfigurieren.

Menüelement	Beschreibung
Aufgaben	Bewegen Sie nach der Auswahl eines verwalteten Produkts/Verzeichnisses den Mauszeiger über diesen Menübefehl, und wählen Sie eine Aufgabe aus, um eine bestimmte Funktion (wie z. B. die Verteilung der neuesten Komponenten) auf einem bestimmten verwalteten Produkt oder einem untergeordneten Server bzw. einer Gruppe von verwalteten Produkten oder untergeordneten Server auszuführen. Sie können eine Aufgabe aus einem Verzeichnis heraus initiieren. Daraufhin sendet Control Manager Anforderungen an alle verwalteten Produkte, die zu diesem Verzeichnis gehören.
Verzeichnisverwaltung	Klicken Sie auf diese Schaltfläche, um das Fenster **Directory Management** zu öffnen. In diesem Fenster können Sie Elemente/ Verzeichnisse verschieben (indem Sie sie ziehen und ablegen) oder neue Verzeichnisse erstellen.
Schaltflächen	
Suchen	Klicken Sie auf diese Schaltfläche, nachdem Sie den Namen eines verwalteten Produkts eingegeben haben, um nach dem angegebenen verwalteten Produkt zu suchen.
Status	Klicken Sie auf diese Schaltfläche, nachdem Sie ein verwaltetes Produkt/ Verzeichnis ausgewählt haben, um Statuszusammenfassungen über das bzw. die verwalteten Produkte im Verzeichnis abzurufen.

MENÜELEMENT	BESCHREIBUNG
Ordner	Klicken Sie auf diese Schaltfläche, nachdem Sie ein Verzeichnis ausgewählt haben, um Statuszusammenfassungen über das bzw. die verwalteten Produkte und die Endpunkte der verwalteten Produkte im Verzeichnis abzurufen.



Hinweis

Sie können verwalteten Produkten, die zu untergeordneten Control Manager Servern gehören, keine Aufgaben vom übergeordneten Control Manager Server zuweisen.

Empfehlungen zur Struktur des Produktverzeichnisses

Bei der Planung der Struktur des Produktverzeichnisses für verwaltete Produkte und untergeordnete Server empfiehlt Trend Micro Folgendes:

TABELLE A-6. Überlegungen zur Gruppierung von verwalteten Produkte oder untergeordneten Servern

STRUKTUR	BESCHREIBUNG
Netzwerk- und Sicherheitsrichtlinien des Unternehmens	Wenn für das Unternehmensnetzwerk unterschiedliche Zugriffs- und Freigaberechte gelten, sollten Sie die verwalteten Produkte und untergeordneten Server entsprechend den Netzwerk- und Sicherheitsrichtlinien des Unternehmens gruppieren.
Organisation und Funktion	Sie können verwaltete Produkte und untergeordnete Server entsprechend den organisatorischen und funktionalen Abteilungen gruppieren. Sie können z. B. zwei Control Manager Server einsetzen, um die Gruppen Produktion und Tests zu verwalten.

STRUKTUR	BESCHREIBUNG
Geografische Lage	Sie können die geografische Lage als Kriterium für die Gruppierung verwenden, wenn der Standort der verwalteten Produkte und untergeordneten Server sich auf die Kommunikation zwischen dem Control Manager Server und seinen verwalteten Produkten oder untergeordneten Server auswirkt.
Verwaltungszuständigkeit	Sie können verwaltete Produkte und untergeordnete Server entsprechend dem System- oder Sicherheitspersonal gruppieren, dem sie zugeordnet sind. Dies ermöglicht die Konfiguration von Gruppen.

Das Produktverzeichnis stellt eine benutzerdefinierte Gruppierung der verwalteten Produkte bereit, durch die Sie in die Lage versetzt werden, die folgenden Funktionen bei der Administrierung von verwalteten Produkten auszuführen:

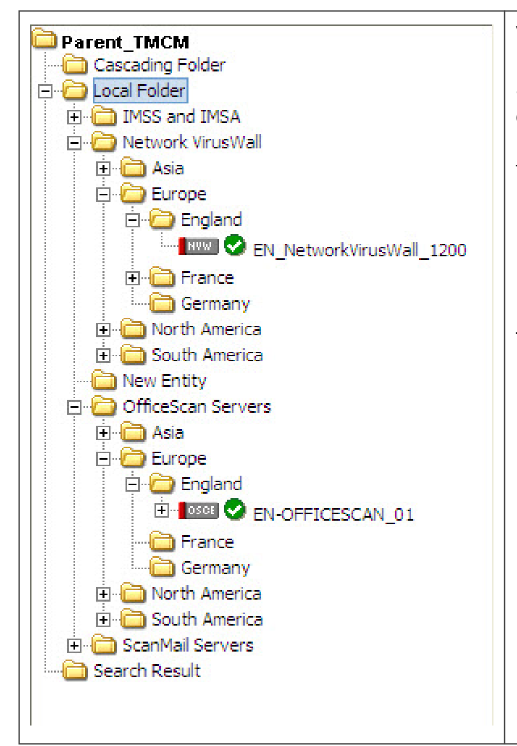
- Verwaltete Produkte konfigurieren
- Produkte anweisen, die Funktion "Jetzt durchsuchen" auszuführen (wenn dieser Befehl unterstützt wird)
- Produktinformationen sowie Details zur Betriebsumgebung anzuzeigen (Beispiel: Produktversion, Pattern-Datei und Scan-Engine-Versionen, Betriebssysteminformationen usw.)
- Protokolle auf Produktebene anzuzeigen
- Viren-Pattern, Scan Engines, Anti-Spam-Regeln und Programmaktualisierungen zu verteilen

Gehen Sie bei der Planung dieser Struktur sorgsam um, denn die Struktur wirkt sich auch auf Folgendes aus:

TABELLE A-7. Überlegungen zur Struktur

ÜBERLEGUNG	WIRKUNG
Benutzerzugriff	Bei der Erstellung von Benutzerkonten fordert der Control Manager zur Eingabe des Produktverzeichnis-Segments auf, auf das der Benutzer Zugriff hat. Mit einer Zugriffsberechtigung auf das Stammsegment erhalten Sie zum Beispiel Zugriff auf das gesamte Verzeichnis. Durch die Gewährung von Zugriff auf ein bestimmtes verwaltetes Produkt erhalten Sie nur Zugriff auf dieses Produkt.
Installation und Verteilung planen	Control Manager verteilt aktualisierte Komponenten (Beispiel: Viren-Pattern-Dateien, Scan Engines, Anti-Spam-Regeln, Programmaktualisierungen) auf Grundlage des Verteilungsplans an die Produkte. Laut diesen Plänen werden die Komponenten an Produktverzeichnisordner und nicht an individuelle Produkte verteilt. Ein gut strukturiertes Verzeichnis erleichtert daher die Festlegung der Empfänger.
Verteilung von Präventionsrichtlinien (OPP) und Damage Cleanup Templates (DCT)	Die OPP- und DCT-Verteilung erfordert Verteilungspläne zur effizienten Verteilung der Präventionsrichtlinie und der Säuberungsaufgaben.

Ein Beispiel für ein Produktverzeichnis sehen Sie weiter unten:



Verwaltete Produkte identifizieren das registrierte Antiviren- und Content-Security-Produkt und stellen außerdem den Verbindungsstatus bereit.



Hinweis

Unabhängig vom Agent-Typ werden neu registrierte verwaltete Produkte im Ordner "Neues Element" angezeigt.

TABELLE A-8. Symbole für verwaltete Produkte

SYMBOL	BESCHREIBUNG
EMAN	InterScan eManager
OSCE	OfficeScan Corporate Edition
SPNT	ServerProtect Information Server
	ServerProtect Domain
NT	ServerProtect for Windows (normaler Server)

SYMBOL	BESCHREIBUNG
	ServerProtect for NetWare (normaler Server)
	InterScan Messaging Security Suite
	InterScan Web Security Suite
	InterScan VirusWall für Windows
	InterScan VirusWall für UNIX
	ScanMail for Microsoft Exchange
	ScanMail für Lotus Notes
	Network VirusWall
	NetScreen Global PRO Firewall
	Symbol für den Verbindungsstatus verwalteter Produkte

Ordnen Sie das Produktverzeichnis mit Hilfe des Directory Managers. Verwenden Sie beschreibende Ordnernamen, um Ihre verwalteten Produkte nach der Art ihres Schutzes und dem Netzwerk-Administrationsmodell von Control Manager zu gruppieren.

Auf das Produktverzeichnis zugreifen

Beim Control Manager Server registrierte verwaltete Produkte werden über das Produktverzeichnis verwaltet.



Hinweis

Die Anzeige und der Zugriff auf Ordner im Produktverzeichnis hängt vom Kontotyp und den Zugriffsrechten des Benutzerkontos ab.

Prozedur

- Klicken Sie im Hauptmenü auf **Products**.

Das Fenster **Product Directory** wird angezeigt.

Komponenten mit dem Produktverzeichnis manuell verteilen

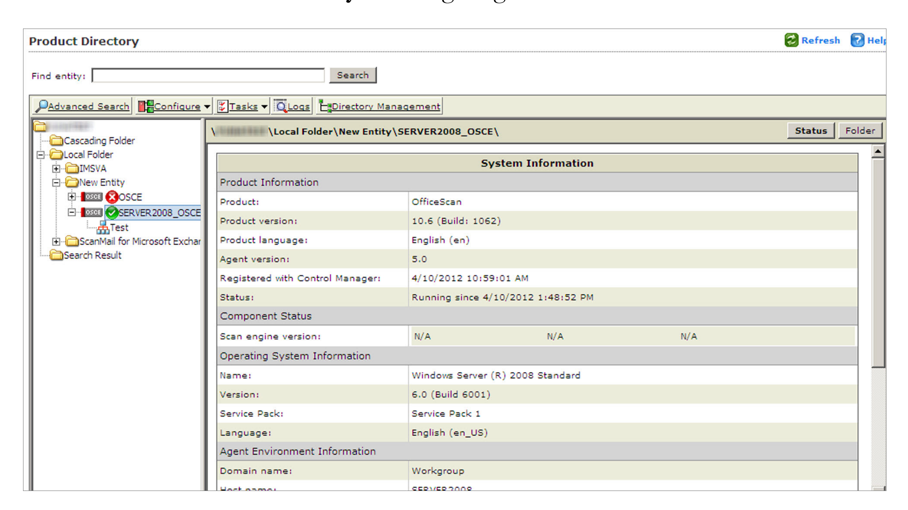
Über manuelle Verteilungen können Sie Viren-Pattern, Spam-Regeln und Scan Engines der verwalteten Produkte bei Bedarf aktualisieren. Setzen Sie diese Methode ein, um Komponenten während eines Virenausbruchs zu aktualisieren.

Laden Sie die neuen Komponenten herunter, bevor Sie Aktualisierungen auf ein bestimmtes verwaltetes Produkt oder Gruppen von verwalteten Produkten verteilen.

Prozedur

1. Klicken Sie im Hauptmenü auf **Products**.

   Das Fenster **Product Directory** wird angezeigt.



2. Wählen Sie ein verwaltetes Produkt oder ein Verzeichnis aus dem Produktverzeichnis.

   Das verwaltete Produkt oder Verzeichnis wird hervorgehoben.

3. Bewegen Sie den Mauszeiger über **Tasks** im Menü "Produktverzeichnis".
4. Wählen Sie aus dem Dropdown-Menü **Deploy <component>**.
5. Klicken Sie auf **Deploy Now**, um die manuelle Verteilung neuer Komponenten zu starten.
6. Überwachen Sie den Fortschritt über das Fenster **Command Tracking**.
7. Klicken Sie im Fenster **Command Tracking** auf den Link "Befehlsdetails", um Details für die Aufgabe "Sofort verteilen" anzuzeigen.

Statuszusammenfassungen für verwaltete Produkte anzeigen

Im Fenster "Produktstatus" werden Zusammenfassungen zu Antivirus, Content-Sicherheit und Web Security für alle verwalteten Produkte angezeigt, die sich in der Struktur des Produktverzeichnisses befinden.

Es gibt zwei Methoden, um die Statuszusammenfassung der verwalteten Produkte anzuzeigen:

- Über das Dashboard mit dem Widget "Ergebnisse der Bedrohungserkennung" (das sich auf der Registerkarte "Zusammenfassung" befindet)
- Über das Produktverzeichnis

Über das Dashboard zugreifen

Prozedur

- Beim Öffnen der Webkonsole von Control Manager wird auf dem Dashboard die Registerkarte **Summary** mit einer Zusammenfassung des gesamten Control Manager Netzwerks angezeigt. Diese Zusammenfassung ist identisch mit der Anzeige auf der Registerkarte Produktstatus im Stammordner des Produktverzeichnisses.

Über das Produktverzeichnis zugreifen

Prozedur

1. Klicken Sie im Hauptmenü auf **Products**.

   Das Fenster **Product Directory** wird angezeigt.

2. Wählen Sie aus der Struktur des Produktverzeichnisses den gewünschten Ordner oder das gewünschte verwaltete Produkt aus.

   - Beim Klicken auf ein verwaltetes Produkt wird auf der Registerkarte "Produktstatus" eine Zusammenfassung des verwalteten Produkts angezeigt.
   - Wenn Sie auf den Stammordner, den Ordner "Neues Element" oder einen anderen benutzerdefinierten Ordner klicken, werden auf der Registerkarte "Produktstatus" die Zusammenfassungen zu Antivirus, Content-Sicherheit und Web Security angezeigt.



Hinweis

Standardmäßig werden im Status Summary die Informationenen einer Woche bis zum Tag Ihrer Abfrage angezeigt. Sie können die Einstellungen **Today**, **Last Week**, **Last Two Weeks** oder **Last Month** unter "Zusammenfassung für Liste anzeigen" ändern.

Verwaltete Produkte konfigurieren

Abhängig von der Produkt- und Agent-Version können Sie das verwaltete Produkt von der Webkonsole des verwalteten Produkts oder über eine von Control Manager generierte Konsole konfigurieren.

Prozedur

1. Klicken Sie im Hauptmenü auf **Products**.

   Das Fenster **Product Directory** wird angezeigt.

2. Wählen Sie das gewünschte verwaltete Produkt aus dem Produktverzeichnis aus.

Der Produktstatus wird im rechten Fensterbereich angezeigt.

3. Bewegen Sie den Mauszeiger über **Configure** im Menü "Produktverzeichnis".

4. Wählen Sie eine der folgenden Optionen:

    - **Configuration Replication**: Das Fenster **Configuration Settings** wird angezeigt.

    a. Wählen Sie den Ordner, in den die Einstellungen des verwalteten Produkts aus dem Produktverzeichnis repliziert werden sollen.

    b. Klicken Sie auf **Replicate**.

    Die Einstellungen des ausgewählten verwalteten Produkts werden auf den verwalteten Zielprodukten repliziert.

    - **<Managed Product Name> Single Sign On**: Die Webkonsole des verwalteten Produkts oder die von Control Manager generierte Konsole wird angezeigt.

    a. Sie können das verwaltete Produkt über die Webkonsole konfigurieren.



Hinweis

Weitere Informationen zur Konfiguration von verwalteten Produkten finden Sie in der Dokumentation des verwalteten Produkts.

Aufgaben für verwaltete Produkte

Mit dem Menübefehl "Aufgaben" rufen Sie die verfügbaren Aktionen für ein bestimmtes verwaltetes Produkt auf. Abhängig vom verwalteten Produkt sind alle oder einige der folgenden Aufgaben verfügbar:

- Engines verteilen und installieren
- Pattern-Dateien/Cleanup-Templates verteilen und installieren
- Programmdateien verteilen und installieren
- Echtzeitsuche aktivieren oder deaktivieren

- Jetzt suchen starten

Sie können die letzten Spam-Regeln, Pattern oder Scan Engines an verwaltete Produkte mit veralteten Komponenten verteilen. Dazu müssen auf dem Control Manager Server die aktuellen, auf dem Trend Micro ActiveUpdate Server verfügbaren Komponenten vorliegen. Stellen Sie dies über einen manuellen Download sicher.

Prozedur

1. Klicken Sie im Hauptmenü auf **Products**.

   Das Fenster **Product Directory** wird angezeigt.

2. Wählen Sie das verwaltete Produkt oder Verzeichnis, um eine Aufgabe zu erteilen.

3. Bewegen Sie den Mauszeiger über **Tasks**.

4. Klicken Sie auf eine Aufgabe aus der Liste. Überwachen Sie den Fortschritt über das Command Tracking. Klicken Sie im angezeigten Fenster auf den Link **Command Details**, um weitere Einzelheiten zum Befehl anzuzeigen.

Protokolle für verwaltete Produkte abfragen und anzeigen

Über die Registerkarte "Protokolle" können Sie die Protokolle für eine Gruppe oder ein bestimmtes verwaltetes Produkt abfragen und anzeigen.

Prozedur

1. Klicken Sie im Hauptmenü auf **Products**.

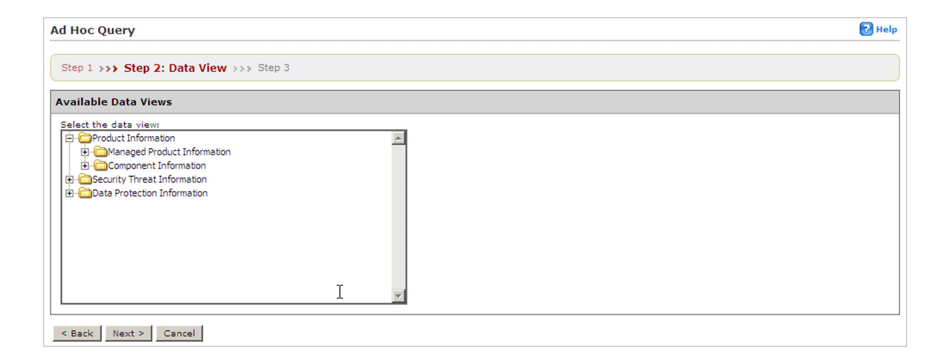
   Das Fenster **Product Directory** wird angezeigt.

2. Wählen Sie das gewünschte verwaltete Produkt oder einen Ordner aus dem Produktverzeichnis.

3. Bewegen Sie den Mauszeiger über **Logs** im Menü "Produktverzeichnis".

4. Klicken Sie im Dropdown-Menü auf **Logs**.

   Das Fenster **Ad Hoc Query > Step 2: Select Data View** wird angezeigt.

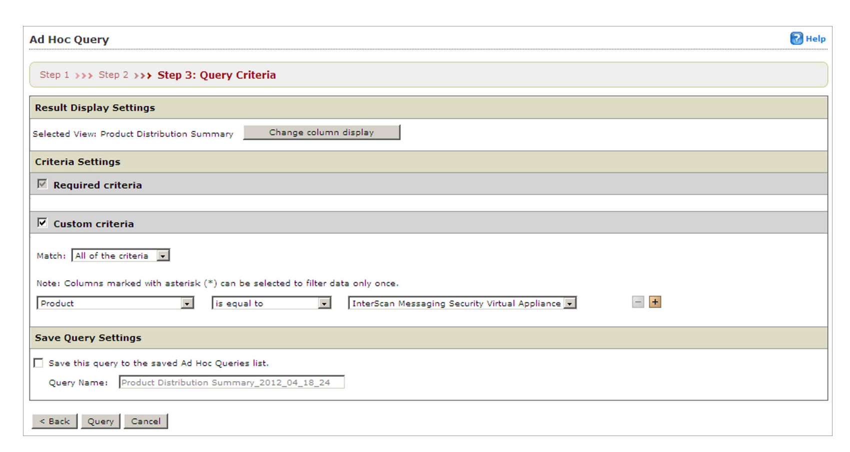


5. Geben Sie die Datenansicht für das Protokoll an:

   a. Wählen Sie die abzufragenden Daten aus dem Bereich "Verfügbare Datenansichten".

   b. Klicken Sie auf **Next**.

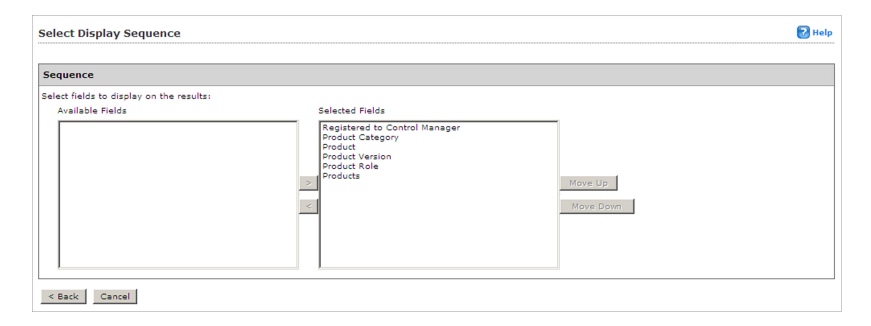
      Das Fenster **Ad Hoc Query > Step 3: Query Criteria** wird angezeigt.



6. Geben Sie die Daten und die Reihenfolge an, in der sie im Protokoll angezeigt werden sollen. Elemente, die oben in der Liste "Ausgewählte Felder" angezeigt werden, werden in der Tabelle in der äußerst linken Spalte angezeigt. Wenn Sie ein Feld aus der Liste "Ausgewählte Felder" entfernen, wird auch die entsprechende Spalte aus der von der Ad-hoc-Abfrage zurückgegebenen Tabelle entfernt.

a. Klicken Sie auf **Change column display**.

Das Fenster **Select Display Sequence** wird angezeigt.



b. Wählen Sie eine Abfragespalte aus der Liste "Verfügbare Felder". Sie können mehrere Elemente durch Drücken der **Shift**- oder **Ctrl**-Taste auswählen.

c. Klicken Sie auf **>**, um Elemente der Liste "Ausgewählte Felder" hinzuzufügen.

d. Legen Sie die Reihenfolge fest, in der Daten angezeigt werden sollen, indem Sie das betreffende Element auswählen und auf **Move up** oder **Move down** klicken.

e. Klicken Sie auf **Back**, wenn die Reihenfolge Ihren Anforderungen entspricht.

7. Geben Sie die Filterkriterien für die Daten an:



Hinweis

Wenn Sie eine Abfrage für zusammenfassende Daten definieren, müssen Sie die Elemente unter "Erforderliche Kriterien" angeben.

- Erforderliche Kriterien:
    - Geben Sie eine Uhrzeit für die Zusammenfassung der Daten an oder legen Sie fest, ob COOKIES in Ihren Berichten erscheinen sollen.
- Benutzerdefinierte Kriterien:

    a. Geben Sie die Regeln für die Filterkriterien für die Datenkategorien an:

- **All of the criteria**: Diese Auswahl dient als logische UND-Funktion. Die im Bericht angezeigten Daten müssen alle Filterkriterien erfüllen.
- **Any of the criteria**: Diese Auswahl dient als logische ODER-Funktion. Die im Bericht angezeigten Daten müssen beliebige Filterkriterien erfüllen.

b. Geben Sie die Filterkriterien für die Daten an. Control Manager unterstützt die Angabe von bis zu 20 Kriterien für die Filterung von Daten.



Tipp

Wenn Sie keine Filterkriterien angeben, gibt die Ad-hoc-Abfrage alle Ergebnisse für die entsprechenden Spalten zurück. Trend Micro empfiehlt die Angabe von Filterkriterien zur Vereinfachung der Datenanalyse, nachdem die Informationen für die Abfrage zurückgegeben wurden.

8. Speichern Sie die Abfrage:

a. Klicken Sie auf **Save this query to the saved Ad Hoc Queries list**.

b. Geben Sie den Namen für die gespeicherte Abfrage in das Feld **Query Name** ein.

9. Klicken Sie auf **Query**.

Das Fenster **Results** wird angezeigt.

10. Speichern Sie den Bericht als .CSV-Datei:

a. Klicken Sie auf **Export to CSV**.

b. Klicken Sie auf **Download**.

c. Geben Sie den Speicherort für die Datei an.

d. Klicken Sie auf **Save**.

11. Speichern Sie den Bericht als .XML-Datei:

a. Klicken Sie auf **Export to XML**.

b. Klicken Sie auf **Download**.

c. Geben Sie den Speicherort für die Datei an.

d. Klicken Sie auf **Save**.



Tipp

Um die Anzahl der in einem Fenster angezeigten Abfrageergebnissen zu erhöhen, wählen Sie einen anderen Wert für " Zeilen pro Seite". In einem einzelnen Fenster können 10, 15, 30 oder 50 Suchabfrageergebnisse pro Seite angezeigt werden.

12. Speichern Sie die Einstellungen für die Abfrage:

a. Klicken Sie auf **Save query settings**.

b. Geben Sie den Namen für die gespeicherte Abfrage in das Feld **Query Name** ein.

c. Klicken Sie auf **OK**.

Die gespeicherte Abfrage wird im Fenster **Saved Ad Hoc Queries** angezeigt.

Informationen zum Wiederherstellen von verwalteten Produkten, die aus dem Produktverzeichnis entfernt wurden

Die folgenden Szenarien können dazu führen, dass der Control Manager verwaltete Produkte aus dem Produktverzeichnis löscht:

- Der Control Manager Server wird neu installiert, und der Befehl **Delete existing records and create a new database** wird ausgewählt

  Bei dieser Option wird eine neue Datenbank mit dem Namen der bestehenden Datenbank erstellt.

- Die beschädigte Control Manager Datenbank wird durch eine andere Datenbank mit dem gleichen Namen ersetzt.

- Das verwaltete Produkt wird versehentlich aus der Verzeichnisverwaltung gelöscht

Auch wenn auf einem Control Manager Server keine Einträge zu verwalteten Produkten mehr angezeigt werden, "wissen" die TMI Agents auf den Produkten trotzdem, wo sie registriert sind. Der Control Manager Agent registriert sich nach acht Stunden oder beim Neustart des Dienstes automatisch erneut.

MCP Agents führen keine automatische Neuregistrierung durch. Administratoren müssen die Neuregistrierung von verwalteten Produkten mit Hilfe von MCP Agents manuell durchführen.

Verwaltete Produkte wiederherstellen, die aus dem Produktverzeichnis entfernt wurden

Prozedur

- Starten Sie den Trend Micro Control Manager Dienst auf dem Server des verwalteten Produkts neu. Weitere Informationen finden Sie unter *Control Manager Dienste anhalten und neu starten auf Seite A-33*.
- Warten Sie, bis der Agent sich erneut registriert hat: Standardmäßig überprüfen ältere Control Manager Agents ihre Verbindung zum Server alle acht Stunden. Wenn der Agent erkennt, dass sein Datensatz gelöscht wurde, registriert er sich automatisch erneut.
- Manuelle Neuregistrierung bei Control Manager: MCP Agents führen keine automatische Neuregistrierung durch und müssen manuell beim Control Manager Server erneut registriert werden.

Control Manager Dienste anhalten und neu starten

Im Fenster **Windows Services** können Sie die folgenden Control Manager Dienste neu starten:

- Trend Micro Management Infrastructure
- Trend Micro Common CGI
- Trend Micro Control Manager



Hinweis

Diese Dienste laufen unter dem Windows-Betriebssystem im Hintergrund. Es handelt sich dabei nicht um Trend Micro Dienste, die einen Aktivierungscode erfordern (Beispiel: Outbreak Prevention Services).

Prozedur

1. Klicken Sie auf **Start** > **Programs** > **Administrative Tools** > **Services**, um das Fenster **Services** zu öffnen.
2. Klicken Sie mit der rechten Maustaste auf **<Control Manager service>**, und klicken Sie anschließend auf **Stop**.
3. Klicken Sie mit der rechten Maustaste auf **<Control Manager service>**, und klicken Sie anschließend auf **Start**.

Nach verwalteten Produkten, Ordnern im Produktverzeichnis oder Computern suchen

Mit Hilfe der Schaltfläche **Search** können Sie im Produktverzeichnis ein bestimmtes verwaltetes Produkt schnell ausfindig machen.

Nach einem Ordner oder verwalteten Produkt suchen

Prozedur

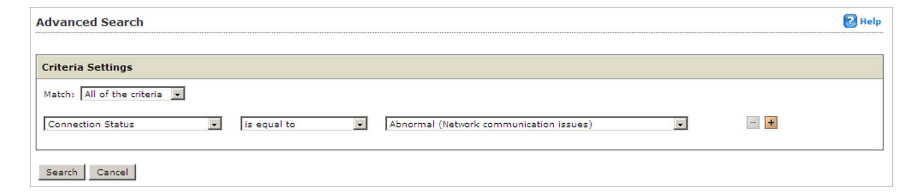
1. Öffnen Sie das Produktverzeichnis.
2. Geben Sie den Anzeigenamen des verwalteten Produkts in das Feld **Find entity** ein.
3. Klicken Sie auf **Search**.

Erweiterte Suche durchführen

Prozedur

1. Öffnen Sie das Produktverzeichnis.
2. Klicken Sie auf **Advanced Search**.

   Das Fenster **Advanced Search** wird angezeigt.

3. Geben Sie die Filterkriterien für das Produkt an. Control Manager unterstützt die Angabe von bis zu 20 Kriterien für die Durchführung von Recherchen.
4. Klicken Sie auf **Search**, um mit der Suche zu beginnen.

   Die Suchergebnisse werden im Produktverzeichnis im Ordner **Search Result** angezeigt.

Das Produktverzeichnis aktualisieren

Prozedur

- Klicken Sie in der rechten oberen Fensterecke im Fenster **Product Directory** auf das Symbol **Refresh**.

Grundlegendes zum Fenster "Verzeichnisverwaltung"

Nach der Registrierung beim Control Manager wird das verwaltete Produkt im Standardordner im Produktverzeichnis angezeigt.

Mit dem Fenster "Verzeichnisverwaltung" können Sie die Struktur des Produktverzeichnisses an Ihre Anforderungen anpassen. Sie können beispielsweise Produkte nach Speicherort oder Produkttyp (Messaging Security, Web Security, Dateispeicherschutz) gruppieren.

Im Produktverzeichnis können Sie Ordner erstellen, ändern oder löschen und verwaltete Produkte von einem Ordner in einen anderen verschieben. Allerdings können Sie den Ordner New entity weder löschen noch umbenennen.

Richten Sie die verwalteten Produkte, die jeweils zu einem Ordner gehört, sorgfältig ein. Berücksichtigen Sie bei der Planung und Implementierung der Struktur Ihrer Ordner und verwalteten Produkte die folgenden Faktoren:

- Produktverzeichnis
- Benutzerkonten
- Verteilungspläne
- Ad-hoc-Abfrage
- Control Manager Berichte

Sie können verwaltete Produkte nach geografischen, administrativen oder produktspezifischen Aspekten gruppieren. In der folgenden Tabelle finden Sie die empfohlenen Gruppierungstypen sowie deren Vor- und Nachteile in Kombination mit verschiedenen Zugriffsrechten zum Zugriff auf verwaltete Produkte oder Ordner im Verzeichnis.

TABELLE A-9. Vergleich der Produktgruppierungen

GRUPPIERUNGSTYP	VORTEILE	NACHTEILE
Geografisch oder administrativ	Klare Struktur	Keine Gruppenkonfiguration für identische Produkte
Produkttyp	Gruppenkonfiguration und Status ist verfügbar	Zugriffsrechte stimmen möglicherweise nicht überein
Kombination von beidem	Gruppenkonfiguration und Verwaltung von Zugriffsrechten	Komplexe Struktur, möglicherweise nicht leicht zu verwalten

Optionen im Fenster "Verzeichnisverwaltung" verwenden

Mit diesen Optionen können Sie verwaltete Produkte in Ihrem Control Manager Netzwerk bearbeiten und organisieren.

Das Fenster **Directory Management** enthält mehrere Optionen:

- Verzeichnisse zum Produktverzeichnis hinzufügen
- Verzeichnisse im Produktverzeichnis umbenennen
- Verwaltete Produkte oder Verzeichnisse im Produktverzeichnis verschieben
- Verwaltete Produkte oder Verzeichnisse aus dem Produktverzeichnis entfernen



Hinweis

Aktivieren Sie das Kontrollkästchen "Berechtigungen beibehalten", wenn der Ordner die Berechtigungen seiner Quelle beim Verschieben behalten soll.

Fenster "Verzeichnisverwaltung" verwenden

Prozedur

- Wählen Sie ein verwaltetes Produkt oder ein Verzeichnis, und klicken Sie auf **Rename**, um das verwaltete Produkt oder das Verzeichnis umzubenennen.
- Klicken Sie auf das **+** oder den Ordner, um die verwalteten Produkte anzuzeigen, die zu einem Ordner gehören.
- Sie können verwaltete Produkte oder Verzeichnisse durch Ziehen in das Produktverzeichnis verschieben.
- Klicken Sie auf **Add Folder** , um dem Produktverzeichnis ein Verzeichnis hinzuzufügen.

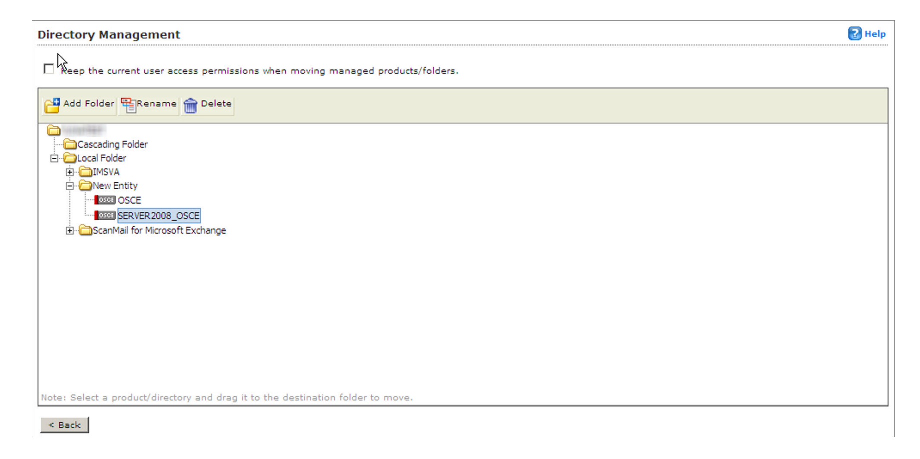
Das Fenster "Verzeichnisverwaltung" öffnen

Im Fenster **Directory Management** gruppieren Sie verwaltete Produkte.

Prozedur

1. Klicken Sie im Hauptmenü auf **Products**.

   Das Fenster **Product Directory** wird angezeigt.



2. Klicken Sie im Menü "Produktverzeichnis" auf **Directory Management**.

   Das Fenster **Directory Management** wird angezeigt.

Ordner erstellen

Sie können die verwalteten Produkte gemäß der Netzwerkverwaltung Ihres Control Managers in verschiedene Ordner gruppieren.

Prozedur

1. Klicken Sie im Hauptmenü auf **Products**.

   Das Fenster **Product Directory** wird angezeigt.

2. Klicken Sie im Menü "Produktverzeichnis" auf **Directory Management**.

   Das Fenster **Directory Management** wird angezeigt.

3. Wählen Sie **Local Folder**.

4. Klicken Sie auf **Add Folder**.

   Das Fenster **Add Directory** wird angezeigt.

5. Geben Sie den Namen für das neue Verzeichnis in das Feld **Directory name** ein.

6. Klicken Sie auf **Save**.



Hinweis

Außer dem Ordner **New Entity** listet der Control Manager alle anderen Ordner in aufsteigender Reihenfolge auf, beginnend mit Sonderzeichen (!, #, $, %, (,), *, +, -, Komma, Punkt, +, ?, @, [,], ^, _, {, |, } und ~), Zahlen (0 bis 9) oder alphabetischen Zeichen (a/A bis z/Z).

Ordner oder verwaltete Produkte umbenennen

Sie können Verzeichnisse und verwaltete Produkte im Fenster **Directory Management** umbenennen.



Hinweis

Bei der Umbenennung eines verwalteten Produkts wird nur der in der Control Manager Datenbank gespeicherte Name geändert; die Umbenennung wirkt sich nicht auf das verwaltete Produkt aus.

Prozedur

1. Klicken Sie im Hauptmenü auf **Products**.

   Das Fenster **Product Directory** wird angezeigt.

2. Klicken Sie im Menü "Produktverzeichnis" auf **Directory Management**.

   Das Fenster **Directory Management** wird angezeigt.

3. Wählen Sie das verwaltete Produkt oder Verzeichnis, das umbenannt werden soll.

4. Klicken Sie auf **Rename**.

   Das Fenster **Rename Directory** wird angezeigt.

5. Geben Sie den Namen für das verwaltete Produkt bzw. Verzeichnis in das Feld **Directory name** ein.

6. Klicken Sie auf **Save**.

7. Klicken Sie auf **OK**.

   Das verwaltete Produkt bzw. Verzeichnis wird unter dem neuen Namen im Produktverzeichnis angezeigt.

Ordner oder verwaltete Produkte verschieben

Achten Sie beim Verschieben von Ordnern besonders auf das Kontrollkästchen **Keep the current user access permissions when moving managed products/folders**. Wenn Sie dieses Kontrollkästchen aktivieren und ein verwaltetes Produkt oder einen Ordner verschieben, behält das verwaltete Produkt oder der Ordner die Berechtigungen des Quellenordners bei. Wenn Sie das Kontrollkästchen deaktivieren und anschließend ein verwaltetes Produkt oder einen Ordner verschieben, übernimmt das verwaltete Produkt oder der Ordner die Zugriffsberechtigungen vom neuen übergeordneten Ordner.

Prozedur

1. Klicken Sie im Hauptmenü auf **Products**.

   Das Fenster **Product Directory** wird angezeigt.

2. Klicken Sie im Menü "Produktverzeichnis" auf **Directory Management**.

   Das Fenster **Directory Management** wird angezeigt.

3. Wählen Sie im Arbeitsbereich den zu verschiebenden Ordner oder das zu verschiebende verwaltete Produkt.

4. Ziehen Sie den Ordner oder das verwaltete Produkt auf den neuen Zielspeicherort.

5. Klicken Sie auf **Save**.

Benutzerdefinierte Ordner löschen

Seien Sie vorsichtig beim Löschen benutzerdefinierter Ordner im Fenster **Directory Management**. Sie könnten versehentlich ein verwaltetes Produkt löschen und damit seine Registrierung beim Control Manager Server rückgängig machen.



Hinweis

Der Ordner **New Entity** kann nicht gelöscht werden.

Prozedur

1. Klicken Sie im Hauptmenü auf **Products**.

   Das Fenster **Product Directory** wird angezeigt.

2. Klicken Sie im Menü "Produktverzeichnis" auf **Directory Management**.

   Das Fenster **Directory Management** wird angezeigt.

3. Wählen Sie das verwaltete Produkt oder Verzeichnis, das gelöscht werden soll.

4. Klicken Sie auf **Delete**.

   Ein Bestätigungsdialogfeld wird angezeigt.

5. Klicken Sie auf **OK**.

6. Klicken Sie auf **Save**.

Neue Komponenten herunterladen und verteilen

Trend Micro empfiehlt die Aktualisierung der Komponenten für Virenschutz und Content-Sicherheit, um vor Gefahren durch aktuelle Viren- und Malware-Bedrohungen geschützt zu sein.

Standardmäßig aktiviert Control Manager nur das Herunterladen von Komponenten, die zu verwalteten Produkten gehören, die im Control Manager Server registriert sind.

Control Manager aktiviert das Herunterladen von Viren-Pattern-Dateien, selbst wenn keine verwalteten Produkte im Control Manager Server registriert sind.

Die folgenden Komponenten sind zu aktualisieren (aufgeführt entsprechend der Häufigkeit der empfohlenen Aktualisierung).

TABELLE A-10. Verfügbare Komponenten

KOMPONENTE	BESCHREIBUNG
Pattern-Dateien/Cleanup-Templates	Pattern-Dateien/Cleanup-Templates enthalten Hunderte von Malware-Signaturen (Beispiel: Viren oder Trojaner) und bestimmen die Fähigkeit des verwalteten Produkts, bösartige Dateiinfektionen zu erkennen und zu säubern
Anti-Spam-Regeln	Bei den Anti-Spam-Regeln handelt es sich um Dateien, die von Trend Micro bereitgestellt werden, und die für die Anti-Spam- und Content-Filterung verwendet werden.
Engines	Engines beziehen sich auf die Scan Engines für Viren/Malware, die Damage Cleanup Engine, die VirusWall Engines, die Spyware/Grayware Engine usw. Diese Komponenten führen die eigentlichen Funktionen zum Suchen und Säubern aus.

KOMPONENTE	BESCHREIBUNG
OfficeScan Plug-in-Programme	OfficeScan Plug-in-Programme (Beispiel: Trend Micro Security for Mac). **Hinweis** Auf der OfficeScan Webkonsole werden alle verfügbaren Plug-in-Programme angezeigt. Sie können angeben, welche der Plug-in-Programme von Control Manager heruntergeladen werden. Möglicherweise wurde jedoch das betreffende Plug-in-Programm nicht von Control Manager heruntergeladen. Das bedeutet, OfficeScan kann das angegebene Plug-in-Programm nicht von Control Manager herunterladen. Überprüfen Sie vor der Angabe eines Plug-in-Programms zum Download vom Control Manager nach OfficeScan, ob Control Manager das Plug-in-Programm bereits heruntergeladen hat.
Produktprogramme und Widget-Pool	Produktspezifische Komponenten (Beispiel: Service-Pack-Veröffentlichungen) und der Control Manager Widget-Pool



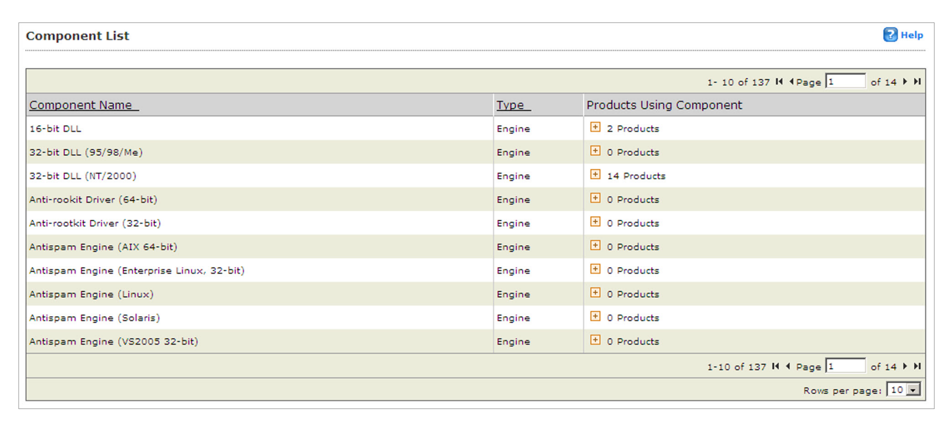
Hinweis

Nur registrierte Benutzer haben ein Anrecht auf Komponenten-Updates.

Um den Netzwerkverkehr von Control Manager zu minimieren, deaktivieren Sie das Herunterladen von Komponenten, für die es kein entsprechendes verwaltetes Produkt gibt.

Das Fenster **Component List** enthält eine vollständige Liste aller Komponenten, die Control Manager für verwaltete Produkte verfügbar hat. In der Liste werden ferner Komponenten mit verwalteten Produkten abgestimmt, die die entsprechende

Komponente verwenden. Klicken Sie auf **Updates** > **Component List**, um das Fenster **Component List** zu öffnen.



Component List

1- 10 of 137 Page 1 of 14

Component Name	Type	Products Using Component
16-bit DLL	Engine	2 Products
32-bit DLL (95/98/Me)	Engine	0 Products
32-bit DLL (NT/2000)	Engine	14 Products
Anti-rookit Driver (64-bit)	Engine	0 Products
Anti-rootkit Driver (32-bit)	Engine	0 Products
Antispam Engine (AIX 64-bit)	Engine	0 Products
Antispam Engine (Enterprise Linux, 32-bit)	Engine	0 Products
Antispam Engine (Linux)	Engine	0 Products
Antispam Engine (Solaris)	Engine	0 Products
Antispam Engine (VS2005 32-bit)	Engine	0 Products

1-10 of 137 Page 1 of 14

Rows per page: 10

ABBILDUNG A-2. Das Fenster "Komponentenliste"

Auf dem Control Manager Server wird nur die letzte Version der Komponente gespeichert. Informationen zum Versionsverlauf einer Komponente finden Sie unter `Stamm>:\Program Files\Trend Micro\Control Manager\AU_log \TmuDump.txt`. `TmuDump.txt` wird generiert, wenn ActiveUpdate-Debugging aktiviert ist.



Tipp

Um den Netzwerkverkehr von Control Manager zu minimieren, deaktivieren Sie das Herunterladen von Komponenten, für die es kein entsprechendes verwaltetes Produkt oder keinen entsprechenden Dienst gibt. Wenn Sie zu einem späteren Zeitpunkt verwaltete Produkte registrieren oder Dienste aktivieren, vergessen Sie nicht, das manuelle oder zeitgesteuerte Herunterladen der entsprechenden Komponenten zu konfigurieren.

Komponenten manuell herunterladen

Laden Sie Komponenten-Updates manuell herunter, wenn Sie den Control Manager zum ersten Mal installieren, wenn Ihr Netzwerk angegriffen wird oder wenn Sie neue Komponenten vor der Verteilung in Ihrem Netzwerk testen möchten.

Trend Micro empfiehlt die folgende Methode zum Konfigurieren von manuellen Downloads. Der manuelle Komponenten-Download erfordert mehrere Schritte:



Tipp

Überspringen Sie Schritt 1 und 2, wenn Sie Ihren Verteilungsplan und Ihre Proxy-Einstellungen bereits konfiguriert haben.

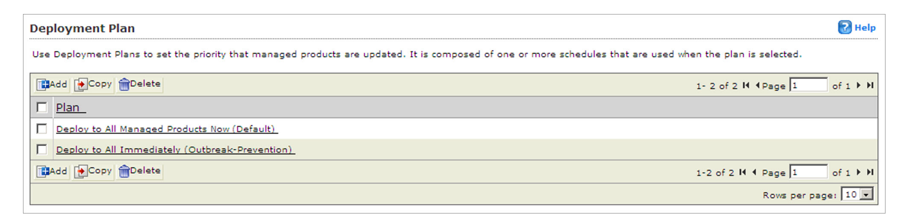
- Schritt 1: Konfigurieren Sie einen Verteilungsplan für Ihre Komponenten.
- Schritt 2: Konfigurieren Sie Ihre Proxy-Einstellungen, wenn Sie einen Proxy-Server verwenden.
- Schritt 3: Wählen Sie die zu aktualisierenden Komponenten.
- Schritt 4: Konfigurieren Sie die Download-Einstellungen.
- Schritt 5: Konfigurieren Sie die Einstellungen für die automatische Verteilung.
- Schritt 6: Schließen Sie den manuellen Download ab.

Schritt 1: Konfigurieren Sie einen Verteilungsplan für Ihre Komponenten.

Prozedur

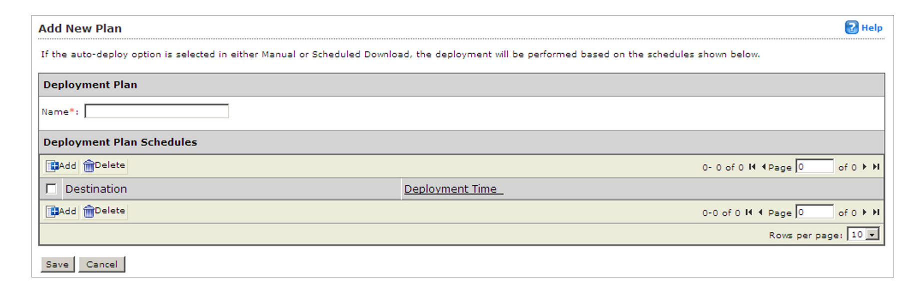
1. Navigieren Sie zu **Updates** > **Deployment Plan**.

   Das Fenster **Deployment Plan** wird angezeigt.



2. Klicken Sie auf **Add**.

   Das Fenster **Add New Plan** wird angezeigt.



3. Geben Sie den Namen eines Verteilungsplans in das Feld **Name** ein.

4. Klicken Sie auf **Add**, um die Details zum Verteilungsplan anzugeben.

   Das Fenster **Add New Schedule** wird angezeigt.



5. Wählen Sie mit einer der folgenden Optionen im Fenster **Add New Schedule** einen Zeitplan für die Verteilung aus:

   - **Start at**: Führt die Verteilung zu einem bestimmten Zeitpunkt aus.

     Geben Sie in den Menüs den Zeitpunkt in Stunden und Minuten an.

   - **Delay**: Nach dem Download der aktuellen Komponenten verzögert Control Manager die Verteilung entsprechend dem von Ihnen angegebenen Intervall.

     Geben Sie in den Menüs die Dauer in Stunden und Minuten an.

6. Wählen Sie im Produktverzeichnis den Ordner, auf den der Zeitplan angewendet werden soll. Control Manager weist den Zeitplan allen Produkten zu, die sich in dem ausgewählten Ordner befinden.

7. Klicken Sie auf **Save**.

   Das Fenster **Add New Plan** wird angezeigt.

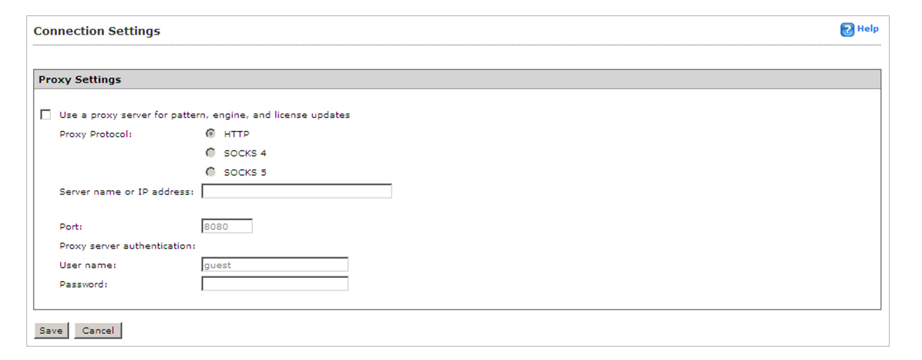
8. Klicken Sie auf **Save**, um den neuen Verteilungsplan zu übernehmen.

Schritt 2: Konfigurieren Sie die Proxy-Einstellungen (wenn Sie einen Proxy-Server verwenden).

Prozedur

1. Navigieren Sie zu **Administration** > **Settings** > **Proxy Settings**.

   Das Fenster **Connection Settings** wird angezeigt.



2. Wählen Sie **Use a proxy server for pattern, engine, and license updates** aus.

3. Wählen Sie das Protokoll:

   - **HTTP**
   - **SOCKS 4**
   - **SOCKS 5**

4. Geben Sie den Host-Namen oder die IP-Adresse des Servers in das Eingabefeld **Server name or IP address** ein.

5. Geben Sie eine Portnummer in das Eingabefeld **Port** ein.

6. Geben Sie einen Anmeldenamen und ein Kennwort ein, wenn Ihr Server eine Authentifizierung erfordert.

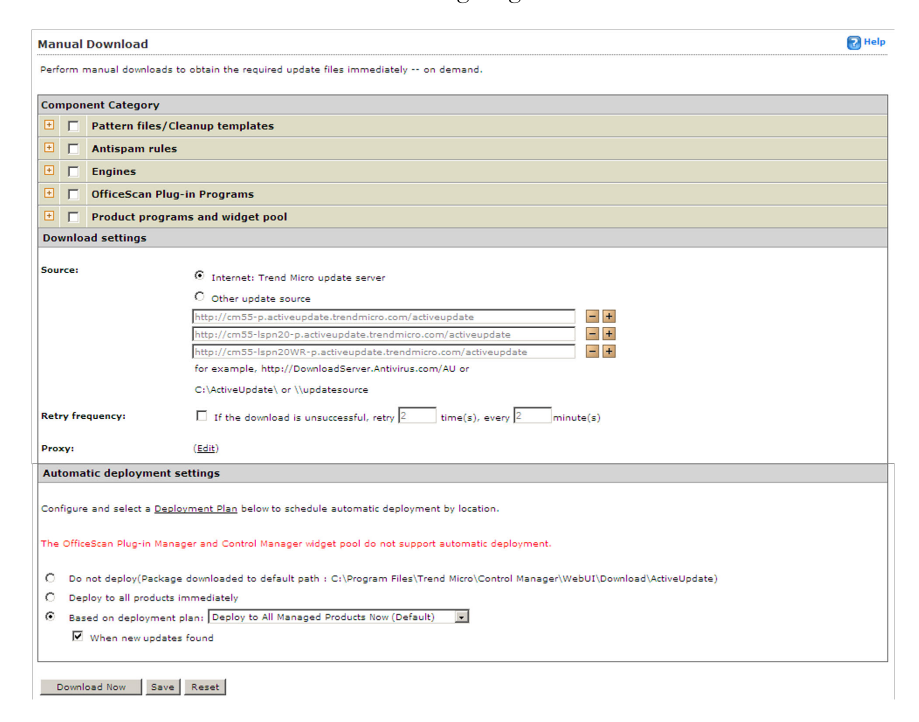
7. Klicken Sie auf **Save**.

Schritt 3: Wählen Sie die zu aktualisierenden Komponenten.

Prozedur

1. Navigieren Sie zu **Updates** > **Manual Download**.

   Das Fenster **Manual Download** wird angezeigt.



2. Wählen Sie im Bereich "Komponentenkategorie" die Download-Komponenten aus.

a. Klicken Sie auf das +-Symbol, um die Komponentenliste für jede Komponentengruppe anzuzeigen.

b. Wählen Sie die gewünschten Komponenten aus. Um alle Komponenten für eine Gruppe auszuwählen, wählen Sie:

- **Pattern files/Cleanup templates**
- **Antispam rules**
- **Engines**
- **OfficeScan Plug-in Programs**
- **Product programs and widget pool**

Schritt 4: Konfigurieren Sie die Download-Einstellungen.

Prozedur

1. Wählen Sie die Update-Adresse aus:

   - **Internet: Trend Micro update server**: Lädt die Komponenten vom offiziellen Trend Micro ActiveUpdate Server herunter.
   - **Other update source**: Geben Sie den URL der Update-Adresse in das zugehörige Eingabefeld ein.

     Unter **Other update source** können Sie mehrere Update-Adressen angeben. Klicken Sie auf das +-Symbol, um eine Update-Adresse hinzuzufügen. Sie können bis zu fünf Update-Adressen konfigurieren.

2. Wählen Sie **Retry frequency**, und geben Sie die Anzahl der Wiederholungen und die Dauer zwischen den Wiederholungen des Komponenten-Downloads an.



Tipp

Klicken Sie auf **Save** und anschließend in diesem Fenster auf **Edit** oder **Deployment Plan**. Ihre Einstellungen werden nur übernommen, wenn Sie auf **Save** klicken.

3. Wenn Sie einen HTTP-Proxy-Server im Netzwerk verwenden (wenn der Control Manager Server keinen direkten Internet-Zugang hat), klicken Sie auf **Edit**, um die Proxy-Einstellungen im Fenster **Connection Settings** zu konfigurieren.

Schritt 5: Konfigurieren Sie die Einstellungen für die automatische Verteilung.

Prozedur

1. Wählen Sie im Bereich "Einstellungen für die automatische Verteilung" einen Verteilungszeitpunkt für die heruntergeladenen Komponenten aus. Wählen Sie zwischen:

    - **Do not deploy**: Die Komponenten werden auf den Control Manager heruntergeladen, aber nicht auf die verwalteten Produkte verteilt. Wählen Sie diese Option unter den folgenden Bedingungen:

        - Individuelle Verteilung auf die verwalteten Produkte

        - Die aktualisierten Komponenten werden vor der Verteilung getestet

    - **Deploy to all products immediately**: Die Komponenten werden auf den Control Manager heruntergeladen und dann auf die verwalteten Produkte verteilt.

    - **Based on deployment plan**: Die Komponenten werden auf den Control Manager heruntergeladen und anhand eines von Ihnen gewählten Zeitplans auf die verwalteten Produkte verteilt.

    - **When new updates found**: Die Komponenten werden auf den Control Manager heruntergeladen, wenn neue Komponenten unter der Update-Adresse verfügbar sind, und anhand eines von Ihnen gewählten Zeitplans auf die verwalteten Produkte verteilt.



Tipp

Klicken Sie auf **Save** und anschließend in diesem Fenster auf **Edit** oder **Deployment Plan**. Ihre Einstellungen werden nur übernommen, wenn Sie auf **Save** klicken.

Schritt 6: Schließen Sie den manuellen Download ab.

Prozedur

1. Kicken Sie auf **Download Now** und bestätigen Sie mit **OK**.

   Das Download-Dialogfenster wird angezeigt. Die Fortschrittsanzeige zeigt den Download-Status an.

2. Klicken Sie auf **Command Details**, um weitere Einzelheiten im Fenster **Command Details** anzuzeigen.

3. Klicken Sie auf **OK**, um zum Fenster **Manual Download** zurückzukehren.

Grundlegendes zu Ausnahmen des zeitgesteuerten Downloads

Mit Hilfe von Download-Ausnahmen kann der Administrator verhindern, dass der Control Manager tagelang oder jeden Tag für eine bestimmte Zeit den Download von Trend Micro Update-Komponenten durchführt.

Diese Funktion ist besonders nützlich, wenn der Administrator die Komponenten-Downloads durch den Control Manager an einem arbeitsfreien Tag oder in der arbeitsfreien Zeit blockieren möchte.



Hinweis

Geplante tägliche Ausnahmen gelten für ausgewählte Tage, während geplante stündliche Ausnahmen für jeden Tag der Woche gelten.

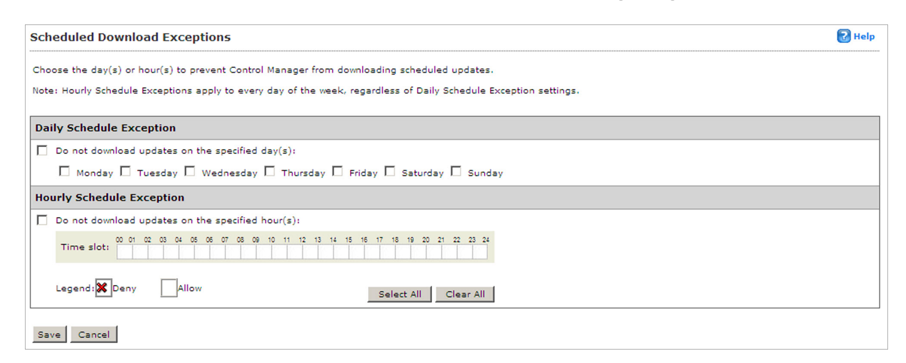
Beispiel: Der Administrator legt fest, dass Control Manager keine Komponenten an Wochenenden oder nach den Geschäftszeiten während der Woche herunterladen soll. Der Administrator aktiviert **Daily Schedule Exception** und wählt **Saturday** und **Sunday**. Der Administrator aktiviert anschließend **Hourly Schedule Exception** und gibt als Stunden **00:00 to 9:00** und **18:00 to 24:00** an.

Ausnahmen des zeitgesteuerten Downloads konfigurieren

Prozedur

1. Navigieren Sie zu **Updates** > **Scheduled Download Exceptions**.

   Das Fenster **Scheduled Download Exceptions** wird angezeigt.



2. Wählen Sie mindestens eine der folgenden Einstellungen:

   - Zur Planung einer täglichen Ausnahme aktivieren Sie im Bereich "Ausnahmen vom Zeitplan (Tage)" einen oder mehrere Tage, an dem bzw. an denen keine Downloads durchgeführt werden, und wählen Sie anschließend **Do not download updates on the specified day(s)**. Jede Woche werden dadurch von Control Manager alle Downloads an den ausgewählten Tagen blockiert.

   - Zur Planung einer stündlichen Ausnahme aktivieren Sie im Bereich "Ausnahmen vom Zeitplan (Stunden)" eine oder mehrere Stunden, an der

bzw. an denen keine Downloads durchgeführt werden, und wählen Sie anschließend **Do not download updates on the specified hour(s)**. Jeden Tag werden dadurch von Control Manager alle Downloads zu den ausgewählten Stunden blockiert.

3. Klicken Sie auf **Save**.

Zeitgesteuerte Downloads konfigurieren

Konfigurieren Sie zeitgesteuerte Komponenten-Downloads, um Ihre Komponenten auf dem neuesten Stand zu halten und Ihr Netzwerk zu schützen. Control Manager unterstützt den Download einzelner Komponenten. Sie können Download-Zeitpläne sowohl für Komponentengruppen als auch für einzelne Komponenten angeben. Alle Zeitpläne sind voneinander unabhängig. Alle Komponenten einer Gruppe werden gemäß einem Download-Zeitplan für diese Komponentengruppe heruntergeladen.

Im Fenster **Scheduled Download** finden Sie folgende Informationen über aktuell in Ihrem Control Manager System vorhandene Komponenten:

- **Zeitintervall**: Zeigt an, wie oft die Komponente aktualisiert wird.
- **Aktiviert**: Zeigt an, ob der Zeitplan für die Komponente aktiviert oder deaktiviert ist.
- **Update-Adresse**: Zeigt den URL bzw. den Pfad der Update-Adresse an.

Die Konfiguration zeitgesteuerter Komponenten-Downloads erfordert mehrere Schritte:

- Schritt 1: Konfigurieren Sie einen Verteilungsplan für Ihre Komponenten.
- Schritt 2: Konfigurieren Sie Ihre Proxy-Einstellungen, wenn Sie einen Proxy-Server verwenden.
- Schritt 3: Wählen Sie die zu aktualisierenden Komponenten.
- Schritt 4: Konfigurieren Sie den Download-Zeitplan.
- Schritt 5: Konfigurieren Sie die Download-Einstellungen.
- Schritt 6: Konfigurieren Sie die Einstellungen für die automatische Verteilung.

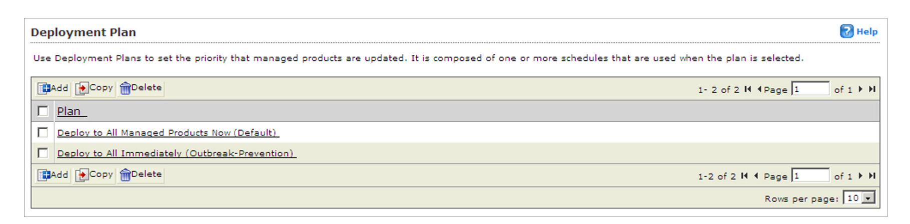
- Schritt 7: Aktivieren Sie den Zeitplan, und speichern Sie die Einstellungen.

Schritt 1: Konfigurieren Sie einen Verteilungsplan für Ihre Komponenten.

Prozedur

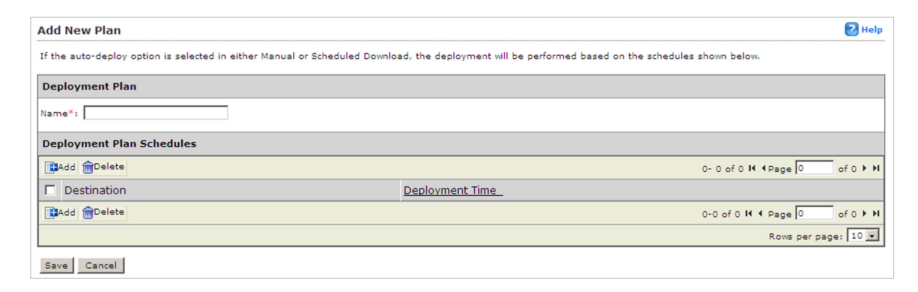
1. Navigieren Sie zu **Updates** > **Deployment Plan**.

   Das Fenster **Deployment Plan** wird angezeigt.



2. Klicken Sie auf **Add**.

   Das Fenster **Add New Plan** wird angezeigt.



3. Geben Sie den Namen eines Verteilungsplans in das Feld **Name** ein.

4. Klicken Sie auf **Add**, um die Details zum Verteilungsplan anzugeben.

   Das Fenster **Add New Schedule** wird angezeigt.



5. Wählen Sie einen Verteilungszeitplan, indem Sie eine der folgenden Optionen auswählen:

   - **Start at**: Führt die Verteilung zu einem bestimmten Zeitpunkt aus.

     Geben Sie in den Menüs den Zeitpunkt in Stunden und Minuten an.

   - **Delay**: Nach dem Download der aktuellen Komponenten verzögert Control Manager die Verteilung entsprechend dem von Ihnen angegebenen Intervall.

     Geben Sie in den Menüs die Dauer in Stunden und Minuten an.

6. Wählen Sie im Produktverzeichnis den Ordner, auf den der Zeitplan angewendet werden soll. Control Manager weist den Zeitplan allen Produkten zu, die sich in dem ausgewählten Ordner befinden.

7. Klicken Sie auf **Save**.

   Das Fenster **Add New Plan** wird angezeigt.

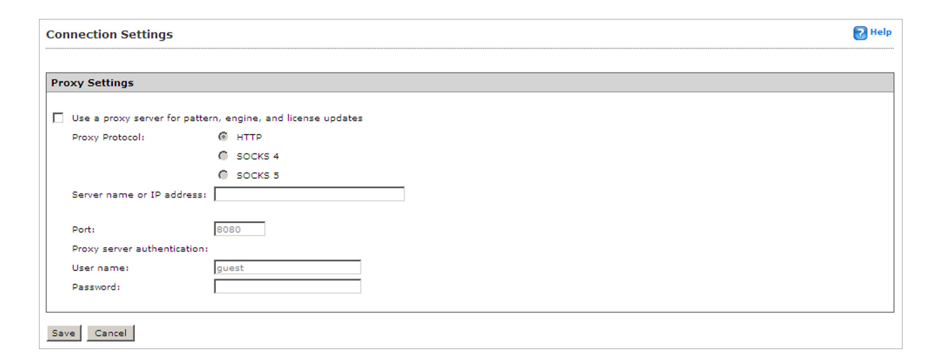
8. Klicken Sie auf **Save**, um den neuen Verteilungsplan zu übernehmen.

Schritt 2: Konfigurieren Sie die Proxy-Einstellungen (wenn Sie einen Proxy-Server verwenden).

Prozedur

1. Navigieren Sie zu **Administration** > **Settings** > **Proxy Settings**.

   Das Fenster **Connection Settings** wird angezeigt.



2. Wählen Sie **Use a proxy server for pattern, engine, and license updates** aus.

3. Wählen Sie das Protokoll:

   - **HTTP**
   - **SOCKS 4**
   - **SOCKS 5**

4. Geben Sie den Host-Namen oder die IP-Adresse des Servers in das Eingabefeld **Server name or IP** ein.

5. Geben Sie eine Portnummer für den Proxy-Server in das Feld **Port** ein.

6. Geben Sie einen Anmeldenamen und ein Kennwort ein, wenn Ihr Server eine Authentifizierung erfordert.

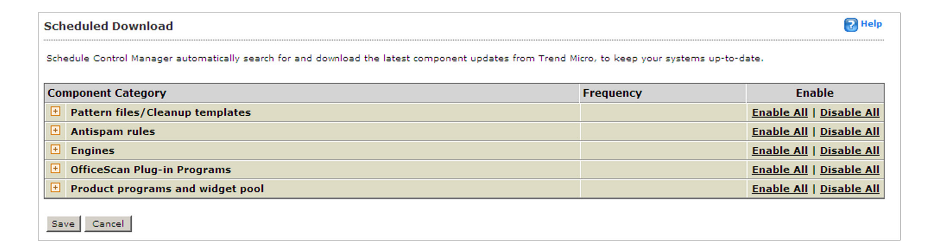
7. Klicken Sie auf **Save**.

Schritt 3: Wählen Sie die zu aktualisierenden Komponenten.

Prozedur

1. Navigieren Sie zu **Updates** > **Scheduled Download**.

   Das Fenster **Scheduled Download** wird angezeigt.



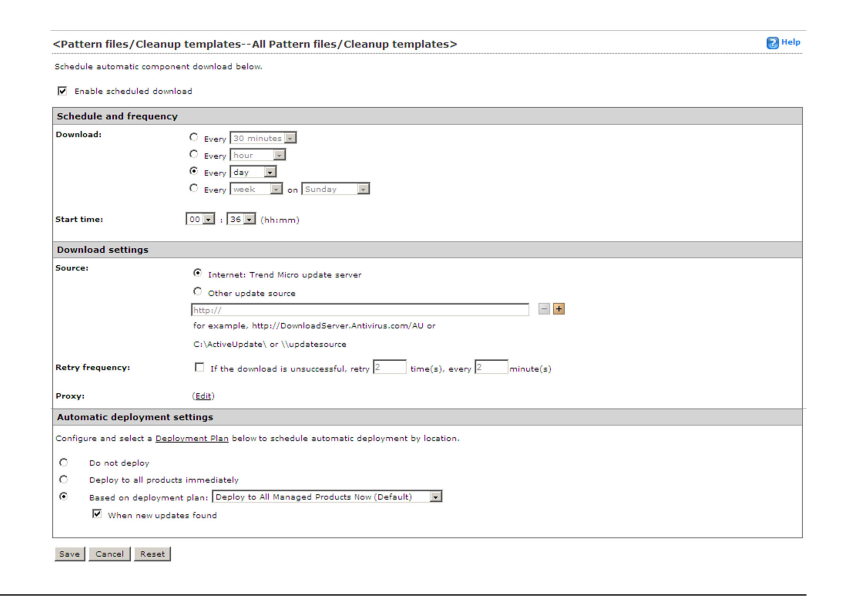
2. Wählen Sie im Bereich "Komponentenkategorie" die Download-Komponenten aus.

   a. Klicken Sie auf das **+**-Symbol, um die Komponentenliste für jede Komponentengruppe anzuzeigen.

   b. Wählen Sie die gewünschten Komponenten aus. Um alle Komponenten für eine Gruppe auszuwählen, wählen Sie:

      - **All Pattern files/Cleanup templates**
      - **All Antispam rules**
      - **All Engines**
      - **OfficeScan Plug-in Programs**
      - **Product programs and widget pool**

      Das Fenster <Komponentenname> wird angezeigt. <Komponentenname> steht für den Namen der ausgewählten Komponente.



Schritt 4: Konfigurieren Sie den Download-Zeitplan.

Prozedur

1. Aktivieren Sie das Kontrollkästchen **Enable scheduled download**, um den zeitgesteuerten Komponenten-Download zu aktivieren.

2. Legen Sie den Download-Zeitplan fest. Wählen Sie ein Intervall aus, und verwenden Sie zur Angabe des gewünschten Zeitplans das entsprechende Listenfeld. Sie können einen Download nach Minuten, Stunden, Tagen oder Wochen planen.

3. Mit dem Menü **Start time** geben Sie an, an welchem Datum und zu welcher Uhrzeit der Zeitplan wirksam wird.

Schritt 5: Konfigurieren Sie die Download-Einstellungen.

Prozedur

1. Wählen Sie die Update-Adresse aus:

   - **Internet**: **Trend Micro update server**: Lädt die Komponenten vom offiziellen Trend Micro ActiveUpdate Server herunter.
   - **Other update source**: Geben Sie den URL der Update-Adresse in das zugehörige Eingabefeld ein.

     Unter **Other update source** können Sie mehrere Update-Adressen angeben. Klicken Sie auf das **+**-Symbol, um eine Update-Adresse hinzuzufügen. Sie können bis zu fünf Update-Adressen konfigurieren.

2. Wählen Sie **Retry frequency**, und geben Sie die Anzahl der Wiederholungen und die Dauer zwischen den Wiederholungen des Komponenten-Downloads an.

   Hinweis

   Klicken Sie auf **Save** und anschließend in diesem Fenster auf **Edit** oder **Deployment Plan**. Ihre Einstellungen werden nur übernommen, wenn Sie auf **Save** klicken.

3. Wenn Sie einen HTTP-Proxy-Server im Netzwerk verwenden (wenn der Control Manager Server keinen direkten Internet-Zugang hat), klicken Sie auf **Edit**, um die Proxy-Einstellungen im Fenster **Connection Settings** zu konfigurieren.

Schritt 6: Konfigurieren Sie die Einstellungen für die automatische Verteilung.

Prozedur

1. Wählen Sie im Bereich "Einstellungen für die automatische Verteilung" einen Verteilungszeitpunkt für die heruntergeladenen Komponenten aus. Wählen Sie zwischen:

- **Do not deploy**: Die Komponenten werden auf den Control Manager heruntergeladen, aber nicht auf die verwalteten Produkte verteilt. Wählen Sie diese Option unter den folgenden Bedingungen:
    - Individuelle Verteilung auf die verwalteten Produkte
    - Die aktualisierten Komponenten werden vor der Verteilung getestet
- **Deploy immediately**: Die Komponenten werden auf Control Manager heruntergeladen und dann auf die verwalteten Produkte verteilt.
- **Based on deployment plan**: Die Komponenten werden auf den Control Manager heruntergeladen und anhand eines von Ihnen gewählten Zeitplans auf die verwalteten Produkte verteilt.
- **When new updates found**: Wenn neue Komponenten unter der Update-Adresse verfügbar sind, werden die Komponenten auf den Control Manager heruntergeladen und an die verwalteten Produkte verteilt.



Hinweis

Klicken Sie auf **Save** und anschließend in diesem Fenster auf **Edit** oder **Deployment Plan**. Ihre Einstellungen werden nur übernommen, wenn Sie auf **Save** klicken.

2. Wählen Sie im Fenster **Deployment Plan** einen Verteilungsplan, nachdem die Komponenten auf Control Manager heruntergeladen wurden.
3. Klicken Sie auf **Save**.

Schritt 7: Aktivieren Sie den Zeitplan, und speichern Sie die Einstellungen.

Prozedur

1. Klicken Sie auf die Schaltfläche "Status" in der Spalte **Enable**.
2. Klicken Sie auf **Save**.

Zeitplan und Häufigkeit für zeitgesteuerte Downloads konfigurieren

Sie können in der Gruppe "Zeitplan und Häufigkeit" angeben, wie oft Control Manager Komponenten-Updates abruft.

Prozedur

1. Navigieren Sie zu **Updates** > **Scheduled Download**.

   Das Fenster **Scheduled Download** wird angezeigt.

2. Wählen Sie im Bereich "Komponentenkategorie" die Download-Komponenten aus.

   a. Klicken Sie auf das **+**-Symbol, um die Komponentenliste für jede Komponentengruppe anzuzeigen.

   b. Wählen Sie die gewünschten Komponenten aus. Um alle Komponenten für eine Gruppe auszuwählen, wählen Sie:

      - **All Pattern files/Cleanup templates**
      - **All Antispam rules**
      - **All Engines**
      - **OfficeScan Plug-in Programs**
      - **Product programs and widget pool**

      Das Fenster <Komponentenname> wird angezeigt. <Komponentenname> steht für den Namen der ausgewählten Komponente.

3. Unter Zeitplan und Häufigkeit:

   a. Legen Sie den Download-Zeitplan fest. Wählen Sie ein Intervall aus, und verwenden Sie zur Angabe des gewünschten Zeitplans das entsprechende Listenfeld. Sie können einen Download nach Minuten, Stunden, Tagen oder Wochen planen.

b. Im Dropdown-Menü **Start time** legen Sie das Datum und die Uhrzeit fest, wann der Zeitplan wirksam wird.

4. Klicken Sie auf **Save**.

Einstellungen für zeitgesteuerte Downloads konfigurieren

In der Gruppe "Download-Einstellungen" können Sie die Komponenten definieren, die Control Manager automatisch herunterlädt, sowie die Download-Methode.

Prozedur

1. Navigieren Sie zu **Updates** > **Scheduled Download**.

   Das Fenster **Scheduled Download** wird angezeigt.

2. Wählen Sie im Bereich "Komponentenkategorie" die Download-Komponenten aus.

   a. Klicken Sie auf das **+**-Symbol, um die Komponentenliste für jede Komponentengruppe anzuzeigen.

   b. Wählen Sie die gewünschten Komponenten aus. Um alle Komponenten für eine Gruppe auszuwählen, wählen Sie:

   - **All Pattern files/Cleanup templates**
   - **All Antispam rules**
   - **All Engines**
   - **OfficeScan Plug-in Programs**
   - **Product programs and widget pool**

     Das Fenster <Komponentenname> wird angezeigt. <Komponentenname> steht für den Namen der ausgewählten Komponente.

3. Wählen Sie unter "Download-Einstellungen" eine der folgenden Update-Adressen:

- **Internet: Trend Micro update server**: (Standardeinstellung) Control Manager lädt die neuesten Komponenten vom Trend Micro ActiveUpdate Server herunter.
- **Other update source**: Ermöglicht die Angabe eines URL für den Speicherort der neuesten Komponentenversion, z. B. der Intranet-Server Ihres Unternehmens.

  Unter **Other update source** können Sie mehrere Update-Adressen angeben. Klicken Sie auf das +-Symbol, um eine zusätzliche Update-Adresse hinzuzufügen. Sie können bis zu fünf Update-Adressen konfigurieren.

4. Wählen Sie **Retry frequency**, um Control Manager anzuweisen, den Download der neuesten Komponenten erneut zu versuchen. In den entsprechenden Feldern können Sie die Anzahl der Versuche und das Intervall zwischen den Versuchen eingeben.



Hinweis

Klicken Sie auf **Save** und anschließend in diesem Fenster auf **Edit** oder **Deployment Plan**. Ihre Einstellungen werden nur übernommen, wenn Sie auf **Save** klicken.

5. Wenn Sie einen HTTP-Proxy-Server im Netzwerk verwenden (wenn der Control Manager Server keinen direkten Internet-Zugang hat), klicken Sie auf **Edit**, um die Proxy-Einstellungen im Fenster **Connection Settings** zu konfigurieren.
6. Klicken Sie auf **Save**.

Automatische Verteilungseinstellungen für den zeitgesteuerten Download konfigurieren

In der Gruppe für die automatischen Verteilungseinstellungen können Sie festlegen, wie Control Manager Aktualisierungen verteilt.

Prozedur

1. Navigieren Sie zu **Updates** > **Scheduled Download**.

   Das Fenster **Scheduled Download** wird angezeigt.

2. Wählen Sie im Bereich "Komponentenkategorie" die Download-Komponenten aus.

   a. Klicken Sie auf das +-Symbol, um die Komponentenliste für jede Komponentengruppe anzuzeigen.

   b. Wählen Sie die gewünschten Komponenten aus. Um alle Komponenten für eine Gruppe auszuwählen, wählen Sie:

      - **All Pattern files/Cleanup templates**
      - **All Antispam rules**
      - **All Engines**
      - **OfficeScan Plug-in Programs**
      - **Product programs and widget pool**

      Das Fenster <Komponentenname> wird angezeigt. <Komponentenname> steht für den Namen der ausgewählten Komponente.

3. Wählen Sie im Bereich "Einstellungen für die automatische Verteilung" einen Verteilungszeitpunkt für die heruntergeladenen Komponenten aus. Wählen Sie zwischen:

   - **Do not deploy**: Die Komponenten werden auf den Control Manager heruntergeladen, aber nicht auf die verwalteten Produkte verteilt. Wählen Sie diese Option unter den folgenden Bedingungen:
     - Individuelle Verteilung auf die verwalteten Produkte
     - Die aktualisierten Komponenten werden vor der Verteilung getestet
   - **Deploy immediately**: Die Komponenten werden auf Control Manager heruntergeladen und dann auf die verwalteten Produkte verteilt.
   - **Based on deployment plan**: Die Komponenten werden auf den Control Manager heruntergeladen und anhand eines von Ihnen gewählten Zeitplans auf die verwalteten Produkte verteilt.
   - **When new updates found**: Die Komponenten werden auf den Control Manager heruntergeladen, wenn neue Komponenten unter der Update-

Adresse verfügbar sind, und anhand eines von Ihnen gewählten Zeitplans auf die verwalteten Produkte verteilt.



Hinweis

Klicken Sie auf **Save** und anschließend in diesem Fenster auf **Edit** oder **Deployment Plan**. Ihre Einstellungen werden nur übernommen, wenn Sie auf **Save** klicken.

4. Wählen Sie im Fenster **Deployment Plan** einen Verteilungsplan, nachdem die Komponenten auf Control Manager heruntergeladen wurden.

5. Klicken Sie auf **Save**.



Hinweis

Die Einstellungen in der Gruppe der automatischen Verteilungseinstellungen gelten nur für Komponenten, die von verwalteten Produkte verwendet werden.

Grundlegendes zu Verteilungsplänen

Mit einem Verteilungsplan können Sie die Reihenfolge festlegen, in der Control Manager Ihre Gruppen von verwalteten Produkten aktualisiert. Mit Control Manager können Sie mehrere Verteilungspläne für unterschiedliche verwaltete Produkte implementieren, die jeweils unterschiedliche Zeitpläne haben. So können Sie beispielsweise während eines Ausbruchs im Zusammenhang mit einem E-Mail-Virus der Aktualisierung der Software-Komponenten für das Durchsuchen von E-Mail-Nachrichten eine höhere Priorität zuweisen, z. B. der letzten Viren-Pattern-Datei für Trend Micro ScanMail für Microsoft Exchange.

Die Control Manager Installation erstellt zwei Verteilungspläne:

- Jetzt an alle verwalteten Produkte verteilen (Standard): Standardplan, der während der Komponenten-Updates verwendet wird
- An alle unverzüglich verteilen (Outbreak-Prevention): Standardplan für die Präventionsphase von Outbreak Prevention Services

Standardmäßig werden auf Grundlage dieser Pläne Updates sofort auf alle Produkte im Produktverzeichnis verteilt.

Wählen Sie oder erstellen Sie Pläne in den Fenstern "Manueller Download" und "Zeitgesteuerter Download". Sie können diese Pläne anpassen oder – entsprechend den Anforderungen in Ihrem Netzwerk – neue erstellen. Erstellen Sie z. B. Verteilungspläne entsprechend der Natur des Ausbruchs:

- E-Mail-Virus
- File-Sharing-Virus

Die Verteilung von Updates an das Produktverzeichnis erfolgt getrennt vom Download-Prozess.

Control Manager lädt die Komponenten herunter und folgt dem Verteilungsplan entsprechend den Einstellungen für manuelle oder zeitgesteuerte Downloads.

Beachten Sie die folgenden Punkte, wenn Sie einen Verteilungsplan erstellen oder implementieren:

- Sie können Verteilungszeitpläne Ordnern, jedoch nicht spezifischen Produkten zuweisen.

  Aus diesem Grund ist die Planung des Inhalts der Produktverzeichnisordner besonders wichtig.

- Sie können nur jeweils einen Ordner für einen Verteilungsplan-Zeitplan festlegen.

  Sie können jedoch mehr als einen Zeitplan pro Verteilungsplan festlegen.

- Control Manager legt die Verzögerungen des Verteilungsplans abhängig von der Ausführungszeit des Downloads fest, und diese Verzögerungen sind unabhängig voneinander.

  Wenn Sie beispielsweise drei Ordner haben, die in Intervallen von 5 Minuten aktualisiert werden sollen, können Sie dem ersten Ordner eine Verzögerung von 5 Minuten zuweisen und anschließend Verzögerungen von 10 und 15 Minuten für die beiden verbleibenden Ordner festlegen.

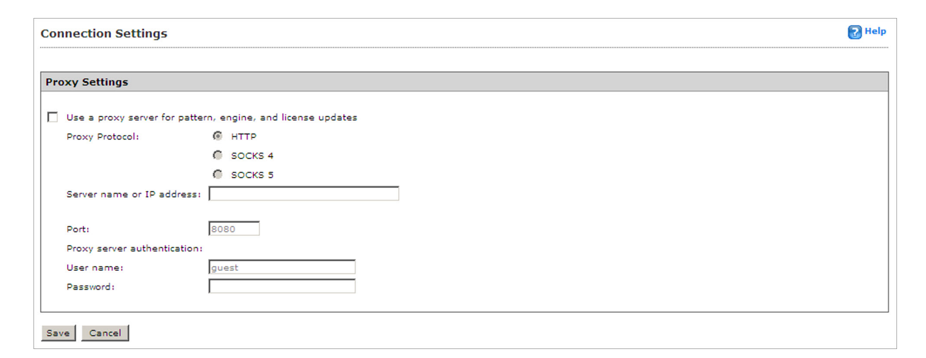
Proxy-Einstellungen konfigurieren

Sie können die Verbindung mit einem Proxy-Server für Komponenten-Downloads und Lizenzaktualisierungen konfigurieren.

Prozedur

1. Navigieren Sie zu **Administration** > **Settings** > **Proxy Settings**.

   Das Fenster **Connection Settings** wird angezeigt.

2. Wählen Sie **Use a proxy server for pattern, engine, and license updates** aus.

3. Wählen Sie das Protokoll:

   - **HTTP**
   - **SOCKS 4**
   - **SOCKS 5**

4. Geben Sie den Host-Namen oder die IP-Adresse des Servers in das Eingabefeld **Server name or IP address** ein.

5. Geben Sie eine Portnummer in das Eingabefeld **Port** ein.

6. Geben Sie einen Anmeldenamen und ein Kennwort ein, wenn Ihr Server eine Authentifizierung erfordert.

7. Klicken Sie auf **Save**.

Aktualisierungs-/Verteilungseinstellungen konfigurieren

Die Verwendung von HTTPS zum Herunterladen von Komponenten vom Trend Micro ActiveUpdate Server (der Standard-Download-Adresse) oder einer anderen Update-Adresse ist eine sicherere Methoden für das Abrufen von Komponenten.

Wenn Komponenten aus einem Freigabeordner in einem Netzwerk heruntergeladen werden, müssen Sie die Authentifizierung für das lokale Windows-Konto und Remote UNC festlegen.

Die lokale Windows-Authentifizierung verweist auf das Active Directory-Benutzerkonto auf dem Control Manager Server. Das Konto sollte über Folgendes verfügen:

- Administratorberechtigung
- Richtlinie *Anmelden als Stapelverarbeitungsauftrag* festgelegt

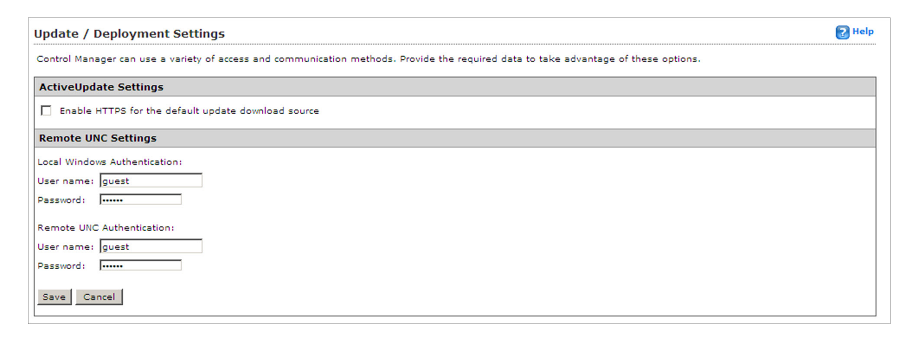
Die Funktion **UNC-Remote-Authentifizierung** verwendet ein Benutzerkonto vom Komponentenquellen-Server mit der Berechtigung, einen Ordner freizugeben, in den Control Manager die Updates herunterladen wird.

HTTPS-Download aktivieren

Prozedur

1. Navigieren Sie zu **Updates** > **Update/Deployment Settings**.

   Das Fenster **Update/Deployment Settings** wird angezeigt.



2. Wählen Sie **Enable HTTPS for the default update download source**.
3. Klicken Sie auf **Save**.
4. Navigieren Sie zum Fenster **Manual Download** oder **Scheduled Download**.
5. Wählen Sie im Arbeitsbereich unter **Download settings Internet: Trend Micro update server**, oder geben Sie den Komponentenquellen-Server Ihres Unternehmens in das Feld **Other update source** ein.
6. Klicken Sie auf **Save**.

UNC-Download aktivieren

Prozedur

1. Navigieren Sie zu **Updates** > **Update/Deployment Settings**.

   Das Fenster **Update/Deployment Settings** wird angezeigt.
2. Geben Sie die Benutzernamen und Kennwörter für die **Local Windows Authentication** und die **Remote UNC Authentication** ein.
3. Klicken Sie auf **Save**.
4. Navigieren Sie zum Fenster **Manual Download** oder **Scheduled Download**.
5. Wählen Sie im Arbeitsbereich unter **Download settings** die Option **Other update source** aus, und geben Sie anschließend einen freigegebenen Netzwerkordner ein.
6. Klicken Sie auf **Save**.

Richtlinie "Anmelden als Stapelverarbeitungsauftrag" einrichten

Die lokale Windows-Authentifizierung verweist auf das Active Directory-Benutzerkonto auf dem Control Manager Server. Das Konto sollte über Folgendes verfügen:

- Administratorberechtigung

- Richtlinie "Anmelden als Stapelverarbeitungsauftrag" festgelegt

---

Prozedur

1. Klicken Sie auf **Start** > **Settings** > **Control Panel**.
2. Klicken Sie auf **Administrative Tools**.
3. Öffnen Sie **Local Security Policy**. Das Fenster "Lokale Sicherheitseinstellungen" wird angezeigt.
4. Klicken Sie auf **Local Polices** > **User Rights Assignment**.
5. Doppelklicken Sie auf **Log on as a batch job**.

   Das Dialogfeld **Log on as a batch job Properties** wird angezeigt.
6. Fügen Sie den Benutzer hinzu, wenn dieser nicht in der Liste angezeigt wird.

Protokolle verwenden

Auch wenn Control Manager Daten von mehreren Protokolltypen empfängt, ermöglicht Control Manager, dass Benutzer Protokolldaten direkt aus der Control Manager Datenbank abrufen. Benutzer können anschließend Filterkriterien angeben, um nur die Daten zusammenzustellen, die sie benötigen.

Control Manager unterstützt auch die Protokollzusammenführung. Die Protokollzusammenführung kann die Abfrageleistung verbessern und die Netzwerkbandbreite reduzieren, die verwaltete Produkte beim Senden von Protokollen an Control Manager benötigen. Dies geschieht jedoch auf Kosten von Daten, die durch die Zusammenführung verloren gehen. Control Manager kann keine Daten abfragen, die in der Control Manager Datenbank nicht vorhanden sind.

Grundlegendes zu Protokollen von verwalteten Produkten

Protokolle von verwalteten Produkten enthalten Informationen über die Leistung der verwalteten Produkte. Sie können Informationen zu bestimmten Produkten oder

Gruppen von Produkten abrufen, die vom übergeordneten oder untergeordneten Server verwaltet werden. Mit der von Control Manager unterstützen Datenabfrage zu Protokollen und den Funktionen zur Datenfilterung können sich Administratoren auf die Informationen konzentrieren, die sie benötigen.



Hinweis

Mehr Protokolle bedeuten reichliche Informationen über das Control Manager Netzwerk. Diese Protokolle belegen jedoch Speicherplatz. Es ist Ihre Aufgabe, einen Ausgleich zwischen dem Bedarf an Informationen und den verfügbaren Systemressourcen zu finden.

Abhängig von ihrer Funktion generieren verwaltete Produkte verschiedene Arten von Protokollen.

TABELLE A-11. Protokolle von verwalteten Produkten

PROTOKOLLKATEGORIE	BESCHREIBUNG
Produktinformationen	Protokolle zu Produktinformationen enthalten Informationen zu Themen wie dem Benutzerzugriff und Ereignissen bei verwalteten Produkte bis hin zur Verteilung von Komponenten und dem Aktualisierungsstatus. • Informationen zu verwalteten Produkten • Versionsinformationen

PROTOKOLLKATEGORIE	BESCHREIBUNG
Informationen zu Sicherheitsbedrohungen	Protokolle zu Sicherheitsbedrohungen enthalten Informationen zu bekannten und potenziellen Sicherheitsbedrohungen, die in Ihrem Netzwerk erkannt wurden. • Viren-/Malware-Informationen • Spyware-/Grayware-Informationen • Informationen zu Content-Verstößen • Informationen zu Spam-Verstößen • Informationen Richtlinien-/Regelverstößen • Informationen zu Web-Verstößen/-Reputation • Informationen zu verdächtigen Bedrohungen • Allgemeine Informationen zu Bedrohungen
Informationen zun Datenschutz	Die Datenschutz-Protokolle enthalten Informationen zu DLP-Vorfällen, Vorlagenübereinstimmungen und Quellen für Vorfälle. • Informationen zur Prävention vor Datenverlust

Protokolldaten abfragen

Ad-hoc-Abfragen bieten Administratoren eine schnelle Methode, um Informationen direkt aus der Control Manager Datenbank abzurufen. Die Datenbank enthält alle Informationen, die von allen Produkten gesammelt wurden, die bei Control Manager Server registriert sind (Protokollzusammenführung kann sich auf die Datenverfügbarkeit der Abfrage auswirken). Ad-hoc-Abfragen stellen ein sehr leistungsfähiges Tool für Administratoren bereit.

Bei der Abfrage von Daten können Administratoren die Abfragekriterien filtern, so dass nur die benötigten Daten zurückgegeben werden. Administratoren können anschließend die Daten zur weiteren Analyse in das CSV- oder XML-Format exportieren oder die Abfrage zur zukünftigen Verwendung speichern. Control Manager unterstützt auch die Freigabe von gespeicherten Abfragen für andere Benutzer, so dass diese von nützlichen Abfragen profitieren.

Füllen Sie die Ad-hoc-Abfrage wie folgt aus:

- Schritt 1: Wählen Sie das verwaltete Produkt oder den aktuellen Control Manager Server für die Abfrage.
- Schritt 2: Wählen Sie die Datenansicht, die abgefragt werden soll.
- Schritt 3: Geben Sie die Filterkriterien sowie die spezifischen Informationen an, die angezeigt werden sollen.
- Schritt 4: Speichern Sie die Abfrage, und führen Sie sie aus.
- Schritt 5: Exportieren Sie die Daten in einer .CSV- oder .XML-Datei.



Hinweis

Control Manager unterstützt die Freigabe von gespeicherten Ad-hoc-Abfragen für andere Benutzer. Gespeicherte und freigegebene Abfragen werden im Fenster **Saved Ad Hoc Queries** angezeigt.

Grundlegendes zu Datenansichten

Bei einer Datenansicht handelt es sich um eine Tabelle, die aus Gruppen verwandter Datenzellen besteht. Datenansichten stellen die Grundlage dar, auf der Benutzer Ad-hoc-Abfragen an die Control Manager Datenbank stellen.

Control Manager ermöglicht direkte Abfragen der Control Manager Datenbank. Datenansichten sind für Berichtvorlagen vom Typ Control Manager 5 und für Ad-hoc-Abfragen verfügbar.

Datenansichten sind Tabellen, die mit Informationen gefüllt sind. Jede Überschrift in einer Datenansicht dient als Spalte in einer Tabelle. Die Dateiansicht "Viren/Malware Aktion/Ergebnis-Zusammenfassung" enthält beispielsweise die folgenden Überschriften:

- Aktionsergebnis
- Durchgeführte Aktion
- Eindeutige Endpunkte
- Eindeutige Quellen

- Funde

Als Tabelle nimmt die Datenansicht das folgende Format mit potenziellen Unterüberschriften unter jeder Überschrift an:

TABELLE A-12. Beispieldatenansicht

AKTIONSERGEBNIS	DURCHGEFÜHRTE AKTION	EINDEUTIGE ENDPUNKTE	EINDEUTIGE QUELLEN	FUNDE

Es ist wichtig, dass Sie sich an diese Informationen erinnern, wenn Sie festlegen, wie Daten in einer Berichtvorlage angezeigt werden.

Control Manager trennt Datenansichten in zwei Hauptkategorien: Produktinformationen und Informationen zu Sicherheitsbedrohungen. Weitere Informationen zu Datenansichten finden Sie im Anhang. Die Hauptkategorien sind ferner in mehrere Unterkategorien unterteilt. Dabei sind die Unterkategorien in zusammenfassende Informationen und detaillierte Informationen unterteilt.

Grundlegendes zu Berichten

Control Manager Berichte bestehen aus zwei Teilen: Berichtvorlagen und Berichtprofile. Während eine Berichtvorlage das Erscheinungsbild des Berichts bestimmt, werden im Berichtprofil der Ursprung der Berichtdaten, der Zeitplan bzw. das Zeitintervall und die Empfänger des Berichts angegeben.

Im Vergleich zu früheren Control Manager Versionen wurden in Control Manager 5.0 radikale Änderungen durch die Einführung angepasster Berichte für Control Manager Administratoren integriert. Control Manager 6.0 unterstützt weiterhin Berichtvorlagen aus früheren Control Manager Versionen, jedoch können Administratoren mit Control Manager 6.0 ihre eigenen angepassten Berichtvorlagen entwickeln.

Grundlegendes zu Control Manager Berichtvorlagen

Eine Berichtvorlage beschreibt das Aussehen des Control Manager Berichtes. Control Manager unterteilt Berichtvorlagen in folgende Typen:

- Control Manager 5 Vorlagen: Benutzerdefinierte Berichtvorlagen, in denen direkte Datenbankabfragen (Datenbankansichten) und Elemente von Berichtvorlagen (Diagramme und Tabellen) verwendet werden. Im Vergleich zu früheren Control Manager Versionen erhalten Benutzer mehr Flexibilität bei der Angabe der Daten, die ihn den Berichten angezeigt werden.
- Control Manager 3 Vorlagen: Enthalten vordefinierte Vorlagen.

Grundlegendes zu Vorlagen für Control Manager 5

Control Manager 5 Berichtvorlagen verwenden Datenbankansichten als Informationsgrundlage für Berichte. Weitere Informationen zu Datenansichten finden Sie unter *Grundlegendes zu Datenansichten auf Seite A-73*. Das Erscheinungsbild der generierten Berichte hängt von den Berichtelementen ab. Berichtelemente bestehen aus dem Folgenden.

TABELLE A-13. Elemente der Control Manager 5 Berichtvorlagen

VORLAGENELEMENT	BESCHREIBUNG
Seitenumbruch	Fügt einen Seitenumbruch in einen Bericht ein. Jede Berichtseite unterstützt bis zu drei Berichtvorlagenelemente.
Statischer Text	Bietet Platz für eine benutzerdefinierte Beschreibung oder Erklärung zum Bericht. Der Inhalt des statischen Textes kann bis zu 4096 Zeichen lang sein.
Balkendiagramm	Fügt ein Balkendiagramm in eine Berichtvorlage ein.
Liniendiagramm	Fügt ein Liniendiagramm in eine Berichtvorlage ein.
Kreisdiagramm	Fügt ein Kreisdiagramm in eine Berichtvorlage ein.
Dynamische Tabelle	Fügt eine dynamische/Kreuztabelle in eine Berichtvorlage ein.
Rastertabelle	Fügt ein Tabelle in eine Berichtvorlage ein. In einer Rastertabelle werden dieselben Informationen angezeigt wie in einer Ad-hoc-Abfrage.

Jede Control Manager 5 Vorlage kann bis zu 100 Berichtvorlagenelemente enthalten. Auf jeder Seite in der Berichtvorlage können sich bis zu drei Berichtvorlagenelemente befinden. Mit Seitenumbrüchen fügen Sie Seiten zu einer Berichtvorlage hinzu.

Damit Sie die Control Manager 5 Berichtvorlagen besser verstehen, stellt Trend Micro die folgenden vordefinierten Berichtvorlagen bereit.



Hinweis

Öffnen Sie das Fenster **Report Templates**, um die vordefinierten Vorlagen von Trend Micro anzuzeigen.

TABELLE A-14. Vordefinierte Control Manager 5 Vorlagen

VORLAGE	BESCHREIBUNG
Zusammenfassung zu erkannten TM-Content-Verstößen	Stellt die folgenden Informationen bereit: • Erkannte Content-Verstöße, gruppiert nach Tag (Liniendiagramm) • Anzahl der Richtlinienverstöße, gruppiert nach Tag (Liniendiagramm) • Anzahl Absender/Benutzer-Verstöße, gruppiert nach Tag (Liniendiagramm) • Anzahl der Empfänger, gruppiert nach Tag (Liniendiagramm) • Die 25 häufigsten Richtlinien mit Verstößen (Balkendiagramm) • Zusammenfassung zu Content-Verstößen - Richtlinie (Rastertabelle) • Die 25 häufigsten Absender/Benutzer mit Verstößen (Balkendiagramm) • Zusammenfassung Content-Verstöße – Absender/ Benutzer mit Verstößen (Rastertabelle) • Zusammenfassung zu Aktionsergebnissen (Kreisdiagramm)

Vorlage	Beschreibung
TM – Status der Verbindung/ Komponenten von verwalteten Produkten	Stellt die folgenden Informationen bereit: • Verbindungsstatus Server/Appliance (Kreisdiagramm) • Verbindungsstatus Client (Kreisdiagramm) • Aktualisierungsstatus Server/Appliance-Pattern-Datei/ Regel (Kreisdiagramm) • Aktualisierungsstatus Client-Pattern-Datei/Regel (Kreisdiagramm) • Aktualisierungsstatus Server/Appliance Scan Engine (Kreisdiagramm) • Aktualisierungsstatus Client Scan Engine (Kreisdiagramm) • Pattern-Datei/Regel-Zusammenfassung für Server/ Appliances (Rastertabelle) • Pattern-Datei/Regel-Zusammenfassung für Clients (Rastertabelle) • Scan Engine-Zusammenfassung für Server/Appliances (Rastertabelle) • Scan Engine-Zusammenfassung für Clients (Rastertabelle)
TM - Allgemeine Zusammenfassung zu Bedrohungen	Stellt die folgenden Informationen bereit: • Zusammenfassung zur vollständigen Risikoanalyse der Netzwerksicherheit (Rastertabelle) • Zusammenfassung Netzwerkschutzgrenze (Rastertabelle) • Informationen zur Analyse von Sicherheitsrisiken für Endpunkte (Rastertabelle) • Informationen zur Analyse von Sicherheitsrisiken für Ziele (Rastertabelle) • Informationen zur Analyse von Sicherheitsrisiken für Quellen (Rastertabelle)

VORLAGE	BESCHREIBUNG
TM - Zusammenfassung zur Spam-Erkennung	Stellt die folgenden Informationen bereit: • Spam-Erkennung, gruppiert nach Tag (Liniendiagramm) • Anzahl der Empfänger-Domänen, gruppiert nach Tag (Liniendiagramm) • Anzahl der Empfänger, gruppiert nach Tag (Liniendiagramm) • Die häufigsten 25 Empfänger-Domänen (Balkendiagramm) • Allgemeine Zusammenfassung zu Spam-Verstößen (Rastertabelle) • Die häufigsten 25 Empfänger von Spam (Balkendiagramm) • Zusammenfassung zu Spam-Empfängern (Rastertabelle)

VORLAGE	BESCHREIBUNG
TM - Zusammenfassung zur Spyware/Grayware-Erkennung	Stellt die folgenden Informationen bereit: • Spyware/Grayware-Erkennung, gruppiert nach Tag (Liniendiagramm) • Anzahl eindeutiger Spyware/Grayware, gruppiert nach Tag (Liniendiagramm) • Anzahl Spyware/Grayware-Quellen, gruppiert nach Tag (Liniendiagramm) • Anzahl Spyware/Grayware-Ziele, gruppiert nach Tag (Liniendiagramm) • Die 25 häufigste Spyware/Grayware (Balkendiagramm) • Allgemeine Zusammenfassung zu Spyware/Grayware (Rastertabelle) • Die 25 häufigsten Spyware/Grayware-Quellen (Balkendiagramm) • Zusammenfassung zu Spyware/Grayware-Quellen (Rastertabelle) • Die 25 häufigsten Spyware/Grayware-Ziele (Balkendiagramm) • Zusammenfassung zu Spyware/Grayware-Zielen (Rastertabelle) • Zusammenfassung zu Aktionsergebnissen (Kreisdiagramm) • Zusammenfassung zu Aktionen/Ergebnissen (Rastertabelle)

VORLAGE	BESCHREIBUNG
TM - Zusammenfassung zur Lösung von verdächtigen Bedrohungen	Stellt die folgenden Informationen bereit: • Erkannte verdächtige Bedrohungen, gruppiert nach Tag (Liniendiagramm) • Anzahl der Regelverstöße, gruppiert nach Tag (Liniendiagramm) • Anzahl der Absender, gruppiert nach Tag (Liniendiagramm) • Anzahl der Empfänger, gruppiert nach Tag (Liniendiagramm) • Anzahl der Quellen-IP-Adressen, gruppiert nach Tag (Liniendiagramm) • Anzahl der Ziel-IP-Adressen, gruppiert nach Tag (Liniendiagramm) • Die 25 häufigsten Absender (Balkendiagramm) • Die 25 häufigsten Empfänger (Balkendiagramm) • Zusammenfassung zu Absendern verdächtiger Bedrohungen (Rastertabelle) • Zusammenfassung zu Empfängern der gefährlichsten verdächtigen Bedrohungen (Rastertabelle) • Die häufigsten 25 Quellen-IP-Adressen (Balkendiagramm) • Die häufigsten 25 Ziel-IP-Adressen (Balkendiagramm) • Zusammenfassung zu den Quellen verdächtiger Bedrohungen (Rastertabelle) • Zusammenfassung zu Zielen der gefährlichsten verdächtigen Bedrohungen (Rastertabelle) • Die 25 häufigsten Protokollnamen (Balkendiagramm) • Zusammenfassung zu Protokollzielen der verdächtigen Bedrohungen (Rastertabelle) • Allgemeine Zusammenfassung zu verdächtigen Bedrohungen (Rastertabelle)

VORLAGE	BESCHREIBUNG
TM - Zusammenfassung zur Viren/Malware-Erkennung	Stellt die folgenden Informationen bereit: • Viren/Malware-Erkennung, gruppiert nach Tag (Liniendiagramm) • Anzahl eindeutiger Viren/Malware, gruppiert nach Tag (Liniendiagramm) • Anzahl der Infektionsziele, gruppiert nach Tag (Liniendiagramm) • Die 25 häufigste Viren/Malware (Balkendiagramm) • Allgemeine Zusammenfassung zu Viren/Malware (Rastertabelle) • Die 25 häufigsten Infektionsquellen (Balkendiagramm) • Zusammenfassung zur Viren/Malware-Infektionsquellen (Rastertabelle) • Die 25 häufigsten Infektionsziele (Balkendiagramm) • Zusammenfassung zu Viren/Malware-Infektionszielen (Rastertabelle) • Zusammenfassung zu Aktionsergebnissen (Kreisdiagramm) • Zusammenfassung zu Viren/Malware (Rastertabelle)

Vorlage	Beschreibung
TM - Zusammenfassung zur Erkennung von Verletzungen durch Internet-Bedrohungen	Stellt die folgenden Informationen bereit: • Erkennung von Verletzungen durch Internet-Bedrohungen, gruppiert nach Tag (Liniendiagramm) • Anzahl der Richtlinienverstöße, gruppiert nach Tag (Liniendiagramm) • Anzahl der Client-Verstöße, gruppiert nach Tag (Liniendiagramm) • Anzahl der URL-Verstöße, gruppiert nach Tag (Liniendiagramm) • Die 25 häufigsten Richtlinien mit Verstößen (Balkendiagramm) • Allgemeine Zusammenfassung zu Erkennung von Verletzungen durch Internet-Bedrohungen (Rastertabelle) • Die 25 häufigsten Clients mit Verstößen (Balkendiagramm) • Zusammenfassung zu Client-IP-Adressen bei Verletzungen durch Internet-Bedrohungen (Rastertabelle) • Die 25 häufigsten URLs mit Verstößen (Balkendiagramm) • Zusammenfassung zu URLs bei Verletzungen durch Internet-Bedrohungen (Rastertabelle) • Zusammenfassung Filter/Sperrtyp (Kreisdiagramm)

Grundlegendes zu Vorlagen für Control Manager 3

Control Manager enthält 87 im Vorfeld generierte Berichtvorlagen, die in sechs Kategorien unterteilt wurden: Kurzfassung, Gateway, Mail-Server, Server, Desktop, Netzwerkprodukte und Prävention vor Datenverlust.



Hinweis

In Control Manager 3.5 gelten Spyware und Grayware nicht mehr als Viren. Diese Änderung wirkt sich auf die Virenanzahl in allen ursprünglichen Virenberichten aus.

Die Berichterstellung kann, je nach Inhalt, einige Sekunden dauern. Sobald der Control Manager einen Bericht fertig gestellt hat, wird das Fenster aktualisiert, und der **View**-Link neben dem Bericht ist verfügbar.

Wählen Sie eine der unten aufgeführten sechs Berichtkategorien aus der Liste "Berichtkategorie" im Fenster "Control Manager" aus:

TABELLE A-15. Kurzfassungen und Berichtstypen

KURZFASSUNGEN	BERICHTTYPEN
Berichte zu Spyware-/Grayware-Funden	• Spyware/Grayware erkannt • Die am häufigsten gefundene Spyware/Grayware (10, 25, 50, 100) • Liste der gefundenen Spyware/ Grayware für alle Elemente
Berichte zu Virenfunden	• Virenfunde • Die am häufigsten gefundenen Viren (10, 25, 50, 100) • Liste der Vireninfektionen für alle Elemente
Vergleichende Berichte	• Spyware/Grayware, gruppiert nach (Tag, Woche, Monat) • Viren, gruppiert nach (Tag, Woche, Monat) • Säuberungsaufgaben, gruppiert nach (Tag, Woche, Monat) • Spam, gruppiert nach (Tag, Woche, Monat)

KURZFASSUNGEN	BERICHTTYPEN
Berichte zu Schwachstellen	• Bewertung der Risikostufe des PCs • Schwachstellenbewertung • Die am häufigsten gesäuberten Infektionen (10, 25, 50, 100) • Potenzielle Schwachstellen, die den größten Schaden anrichten (10, 25, 50, 100) • Schwachstellen nach Risikostufe

TABELLE A-16. Berichte und Berichtstypen für Gateway-Produkte

BERICHTE ZU GATEWAY-PRODUKTEN	BERICHTTYPEN
Berichte zu Spyware-/Grayware-Funden	• Spyware/Grayware erkannt • Die am häufigsten gefundene Spyware/Grayware (10, 25, 50, 100)
Berichte zu Virenfunden	• Virenfunde • Die am häufigsten gefundenen Viren (10, 25, 50, 100)
Vergleichende Berichte	• Spyware/Grayware, gruppiert nach (Tag, Woche, Monat) • Spam, gruppiert nach (Tag, Woche, Monat) • Viren, gruppiert nach (Tag, Woche, Monat)
Berichte zur Verteilungsrate	• Detaillierte Zusammenfassung • Grundlegende Zusammenfassung • Detaillierte Zusammenfassung zur Durchfallquote • OPS-Verteilungsrate für IMSS

Tabelle A-17. Berichte und Berichtstypen für Mail-Server-Produkte

Berichte zu Mail-Server-Produkten	Berichttypen
Berichte zu Spyware-/Grayware-Funden	• Spyware/Grayware erkannt • Die am häufigsten gefundene Spyware/Grayware (10, 25, 50, 100)
Berichte zu Virenfunden	• Virenfunde • Absender mit den meisten infizierten E-Mails (10, 25, 50, 100) • Die am häufigsten gefundenen Viren (10, 25, 50, 100)
Vergleichende Berichte	• Spyware/Grayware, gruppiert nach (Tag, Woche, Monat) • Viren, gruppiert nach (Tag, Woche, Monat)
Berichte zur Verteilungsrate	• Detaillierte Zusammenfassung • Grundlegende Zusammenfassung • Detaillierte Zusammenfassung zur Durchfallquote

Tabelle A-18. Berichte und Berichtstypen für serverbasierte Produkte

Berichte zu serverbasierten Produkten	Berichttypen
Berichte zu Spyware-/Grayware-Funden	• Spyware/Grayware erkannt • Die am häufigsten gefundene Spyware/Grayware (10, 25, 50, 100)
Berichte zu Virenfunden	• Virenfunde • Die am häufigsten gefundenen Viren (10, 25, 50, 100)

Berichte zu serverbasierten Produkten	Berichttypen
Vergleichende Berichte	• Spyware/Grayware, gruppiert nach (Tag, Woche, Monat) • Viren, gruppiert nach (Tag, Woche, Monat)
Berichte zur Verteilungsrate	• Detaillierte Zusammenfassung • Grundlegende Zusammenfassung • Detaillierte Zusammenfassung zur Durchfallquote

Tabelle A-19. Berichte und Berichtstypen für Desktop-Produkte

Berichte zu Desktop-Produkten	Berichttypen
Berichte zu Spyware-/Grayware-Funden	• Spyware/Grayware erkannt • Am häufigsten erkannte Spyware/ Grayware (10, 25, 50,100)
Berichte zu Virenfunden	• Virenfunde • Am häufigsten erkannte Viren (10, 25, 50,100)
Berichte zu OfficeScan Client-Informationen	• Detaillierte Zusammenfassung • Grundlegende Zusammenfassung
Bericht zur OfficeScan Produktregistrierung	Registrierungsstatus
Vergleichende Berichte	• Spyware/Grayware, gruppiert nach (Tag, Woche, Monat) • Viren, gruppiert nach (Tag, Woche, Monat)
Berichte zur OfficeScan Server Verteilung	• Detaillierte Zusammenfassung • Grundlegende Zusammenfassung • Detaillierte Zusammenfassung zu Durchfallquoten

BERICHTE ZU DESKTOP-PRODUKTEN	BERICHTTYPEN
Berichte zu Damage Cleanup Services von OfficeScan	• Detaillierte Zusammenfassung • Die am häufigsten gesäuberten Infektionen (10, 25, 50, 100)

TABELLE A-20. Berichte und Berichtstypen für Netzwerkprodukte

BERICHTE ZU NETZWERKPRODUKTEN	BERICHTTYPEN
Berichte zu Network VirusWall	• Bericht zu Richtlinienverstößen, gruppiert nach (Tag, Woche, Monat) • Die am häufigsten gefundenen Clients mit Verstößen (10, 25, 50, 100) • Bericht zu Serviceverstößen, gruppiert nach (Tag, Woche, Monat)
Appliance-Berichte zu Trend Micro Total Discovery	• Zusammenfassung zu Vorfällen, gruppiert nach (Tag, Woche, Monat) • Clients mit hohem Risiko (10, 25, 50, 100) • Bericht mit Zusammenfassung bekannter und unbekannter Risiken

TABELLE A-21. Berichte und Berichtstypen zu Prävention vor Datenverlust

BERICHTE ZUR PRÄVENTION VOR DATENVERLUST	BERICHTTYPEN
Wichtigste Quellen für DLP-Vorfälle	• Vorfälle nach Absender (10, 20, 30, 40, 50) • Vorfälle nach Host-Name (10, 20, 30, 40, 50) • Vorfälle nach Empfänger (10, 20, 30, 40, 50) • Vorfälle nach Quellen-IP-Adresse (10, 20, 30, 40, 50) • Vorfälle nach URL (10, 20, 30, 40, 50) • Vorfälle nach Benutzer (10, 20, 30, 40, 50) • Wichtigste Vorlagenübereinstimmungen (10, 20, 30, 40, 50) • Verteilung der Vorfälle nach Kanal • Vorfalltrend, gruppiert nach (Tag, Woche, Monat) • Vorfälle nach Kanal, gruppiert nach (Tag, Woche, Monat)

Berichte zur Prävention vor Datenverlust	Berichttypen
Signifikanter Anstieg von Vorfällen	• Signifikanter Anstieg von Vorfällen (%) nach Kanal (10, 20, 30, 40, 50) • Signifikanter Anstieg von Vorfällen nach Kanal (10, 20, 30, 40, 50) • Signifikanter Anstieg von Vorfällen (%) nach Absender (10, 20, 30, 40, 50) • Signifikanter Anstieg von Vorfällen nach Absender (10, 20, 30, 40, 50) • Signifikanter Anstieg von Vorfällen (%) nach Host-Name (10, 20, 30, 40, 50) • Signifikanter Anstieg von Vorfällen nach Host-Name (10, 20, 30, 40, 50) • Signifikanter Anstieg von Vorfällen (%) nach Benutzer (10, 20, 30, 40, 50) • Signifikanter Anstieg von Vorfällen nach Benutzer (10, 20, 30, 40, 50) • Signifikanter Anstieg von Vorfällen (%) nach Quellen-IP-Adresse (10, 20, 30, 40, 50) • Signifikanter Anstieg von Vorfällen nach Quellen-IP-Adresse (10, 20, 30, 40, 50) • Signifikanter Anstieg von Vorfällen (%) nach Vorlage (10, 20, 30, 40, 50) • Signifikanter Anstieg von Vorfällen nach Vorlage (10, 20, 30, 40, 50)

Einzelberichte hinzufügen

Sie können mit Control Manager Einzelberichte über die Berichtvorlagen Control Manager 3 und Control Manager 5 generieren. Benutzer müssen die Berichtvorlagen vom Typ Control Manager 5 erstellen, während Trend Micro die Berichtvorlagen vom

Typ Control Manager 3 erstellt hat. Die Arbeitsschritte zum Erstellen eines Einzelberichts ähneln sich für alle Berichtstypen und umfassen Folgendes:

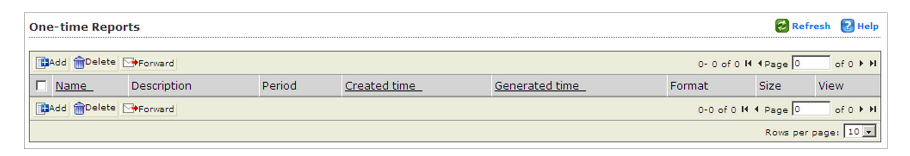
1. Öffnen Sie das Fenster **Add One-time Report**, und wählen Sie den Berichttyp.
2. Geben Sie das bzw. die Produkte an, aus denen die Berichtsdaten generiert werden:
3. Geben Sie das Datum an, an dem das bzw. die Produkte die Daten erzeugen soll.
4. Geben Sie den Empfänger des Berichts an.

Schritt 1: Öffnen Sie das Fenster "Einzelbericht hinzufügen", und wählen Sie den Berichttyp.

Prozedur

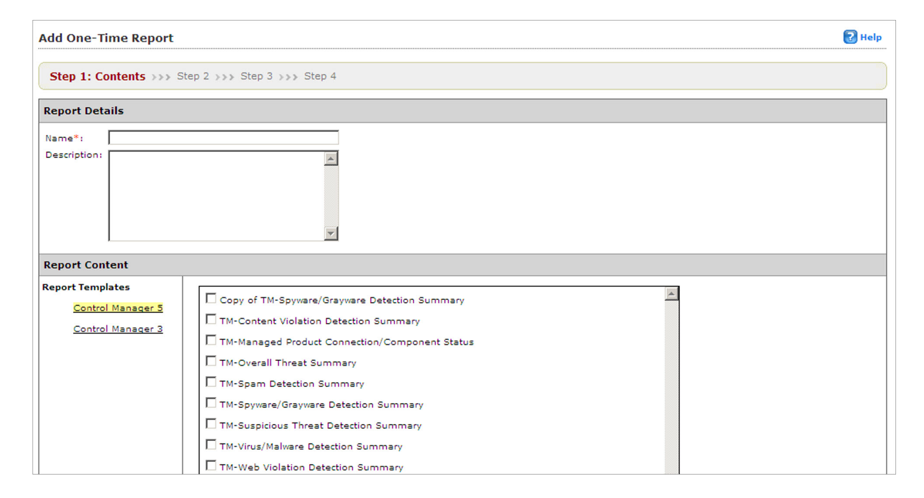
1. Navigieren Sie zu **Reports** > **One-time Reports**.

   Das Fenster **One-time Reports** wird angezeigt.

2. Klicken Sie auf **Add**.

   Das Fenster **Add One-time Report > Step 1: Contents** wird angezeigt.



3. Geben Sie einen Namen für den Bericht unter "Berichtdetails" in das Feld **Name** ein.

4. Geben Sie eine Beschreibung für den Bericht unter "Berichtdetails" in das Feld **Description** ein.

5. Wählen Sie die Control Manager Vorlage, anhand der der Bericht generiert werden soll:

   - **Berichtvorlage Control Manager 5**:

     a. Wählen Sie die Control Manager 5 Vorlage, anhand der der Bericht generiert werden soll: Wenn die vorhandenen Berichte Ihre Anforderungen nicht erfüllen, erstellen Sie eine neue Vorlage über das Fenster **Report Templates**.

   - **Berichtvorlage Control Manager 3**:

     a. Klicken Sie unter Berichtinhalt auf **Control Manager 3**. Die Control Manager 3 Vorlagen werden im Arbeitsbereich auf der rechten Seite unter "Berichtinhalt" angezeigt.

     b. Wählen Sie die Berichtkategorie, die als Grundlage für den Bericht dient.

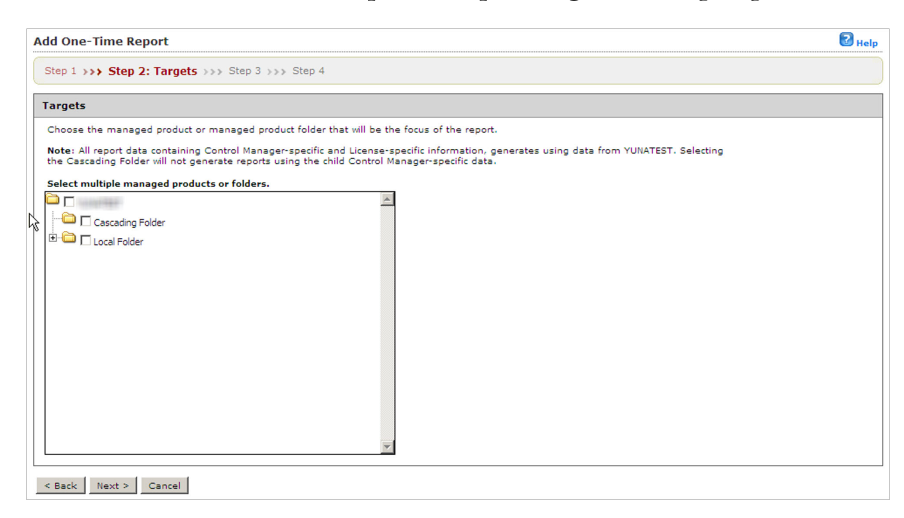
     c. Wählen Sie die Control Manager 3 Vorlagendaten, auf denen die Vorlage basiert.

6. Wählen Sie das Format für den generierten Bericht:

   - **Berichtformate für Control Manager 5**:
     - Adobe PDF Format (*.pdf)
     - HTML-Format (*.html)
     - XML-Format (*.xml)
     - CSV-Format (*.csv)
   - **Berichtformate für Control Manager 3**:
     - Rich Text Format (*.rtf)
     - Adobe PDF Format (*.pdf)
     - ActiveX
     - Crystal Report Format (*.rpt)

7. Klicken Sie auf **Next**.

   Das Fenster **Add One-Time Report > Step 2: Targets** wird angezeigt.



Schritt 2: Geben Sie das bzw. die Produkte an, aus denen die Berichtsdaten generiert werden:

Prozedur

1. Wählen Sie das verwaltete Produkt oder Verzeichnis, aus dem Control Manager die Berichtinformationen erfasst.
2. Wenn der Bericht Daten von einem Network VirusWall Enforcer Gerät enthält, geben Sie die Clients für die Berichtgenerierung an:
    - **All clients**: Berichte werden von allen Network VirusWall Enforcer Geräten generiert
    - **IP range**: Berichte werden auf Grundlage eines bestimmten IP-Adressbereichs generiert
    - **Segment**: Berichte werden auf Grundlage eines bestimmten Netzwerksegments generiert
3. Klicken Sie auf **Next**.

Schritt 3: Geben Sie das Datum an, an dem das bzw. die Produkte die Daten erzeugen soll.

Prozedur

1. Geben Sie das Datum an, an dem die Daten generiert werden sollen:
    - Wählen Sie aus dem Listenfeld eine der folgenden Optionen aus:
        - Gesamter Zeitraum
        - Letzte 24 Stunden
        - Heute
        - Letzte 7 Tage
        - Letzte 14 Tage

    - Letzte 30 Tage

- Geben Sie einen Datumsbereich an:

    - Geben Sie ein Datum in das Feld **From** ein.
    - Geben Sie eine Uhrzeit in die betreffenden Felder **hh** und **mm** ein.
    - Geben Sie ein Datum in das Feld **To** ein.
    - Geben Sie eine Uhrzeit in die betreffenden Felder **hh** und **mm** ein.



Hinweis

Klicken Sie auf das Kalendersymbol neben den Feldern **From** und **To**, um den Datumsbereich über den dynamischen Kalender festzulegen.

2. Klicken Sie auf **Next**.

Schritt 4: Geben Sie den Empfänger des Berichts an:

Prozedur

1. Geben Sie eine Betreffzeile für die E-Mail-Nachricht mit dem Bericht in das Feld **Subject** ein.
2. Geben Sie eine Beschreibung des Berichts in das Feld **Message** ein.
3. Wählen Sie **Email the report as an attachment**, um den Bericht an den angegebenen Empfänger zu versenden.
4. Aktivieren Sie diese Option, um Benutzer oder Gruppen aus der Liste **Report Recipients** auszuwählen.
5. Wählen Sie die Benutzer/Gruppen, die den Bericht erhalten sollen, und klicken Sie auf die Schaltfläche **>>**.
6. Klicken Sie auf **Finish**, nachdem Sie alle Benutzer/Gruppen ausgewählt haben, die den Bericht erhalten sollen.

Zeitgesteuerte Berichte hinzufügen

Sie können mit Control Manager zeitgesteuerte Berichte über die Berichtvorlagen Control Manager 3 und Control Manager 5 generieren. Benutzer müssen die Berichtvorlagen vom Typ Control Manager 5 erstellen, während Trend Micro die Berichtvorlagen vom Typ Control Manager 3 erstellt hat. Die Schritte zum Erstellen eines zeitgesteuerten Berichts ähneln sich für alle Berichtstypen:

1. Öffnen Sie das Fenster **Add Scheduled Report**, und wählen Sie den Berichttyp.
2. Geben Sie das bzw. die Produkte an, aus denen die Berichtsdaten generiert werden:
3. Geben Sie das Datum an, an dem das bzw. die Produkte die Daten erzeugen soll.
4. Geben Sie den Empfänger des Berichts an.

Schritt 1: Öffnen Sie das Fenster "Zeitgesteuerten Bericht hinzufügen", und wählen Sie den Berichttyp.

Prozedur

1. Navigieren Sie zu **Reports** > **Scheduled Reports**.
2. Klicken Sie auf **Add**.
3. Geben Sie einen Namen für den Bericht in das Feld **Name** ein.
4. Geben Sie eine aussagekräftige Beschreibung für den Bericht in das Feld **Description** ein.
5. Wählen Sie die Control Manager Vorlage, anhand der der Bericht generiert werden soll:
    - Berichtvorlage Control Manager 5:
        a. Wählen Sie die Control Manager 5 Vorlage, anhand der der Bericht generiert werden soll: Wenn die vorhandenen Berichte Ihre Anforderungen nicht erfüllen, erstellen Sie eine neue Vorlage über das Fenster "Berichtvorlagen".
    - Berichtvorlage Control Manager 3:

a. Klicken Sie unter Berichtinhalt auf **Control Manager 3**. Die Control Manager 3 Vorlagen werden im Arbeitsbereich auf der rechten Seite unter "Berichtinhalt" angezeigt.

b. Wählen Sie die Berichtkategorie, die als Grundlage für den Bericht dient.

c. Wählen Sie die Control Manager 3 Vorlagendaten, auf denen die Vorlage basiert.

6. Wählen Sie das Format für den generierten Bericht:

- Berichtformate für Control Manager 5:
  - Adobe PDF Format (*.pdf)
  - HTML-Format (*.html)
  - XML-Format (*.xml)
  - CSV-Format (*.csv)
- Berichtformate für Control Manager 3:
  - Rich Text Format (*.rtf)
  - Adobe PDF Format (*.pdf)
  - ActiveX
  - Crystal Report Format (*.rpt)

7. Klicken Sie auf **Next**.

Schritt 2: Geben Sie das bzw. die Produkte an, aus denen die Berichtsdaten generiert werden.

Prozedur

1. Wählen Sie das verwaltete Produkt oder Verzeichnis, aus dem Control Manager die Berichtinformationen erfasst.

2. Wenn der Bericht Daten von einem Network VirusWall Enforcer Gerät enthält, geben Sie die Clients für die Berichtgenerierung an:

    - **All clients**: Berichte werden von allen Network VirusWall Enforcer Geräten generiert

    - **IP range**: Berichte werden auf Grundlage eines bestimmten IP-Adressbereichs generiert

    - **Segment**: Berichte werden auf Grundlage eines bestimmten Netzwerksegments generiert

3. Klicken Sie auf **Next**.

Schritt 3: Geben Sie das Datum an, an dem das bzw. die Produkte die Daten erzeugen soll.

Prozedur

1. Geben Sie an, wie oft die Berichte generiert werden sollen:

    - **Daily**: Berichte werden täglich generiert.

    - **Weekly**: Berichte werden wöchentlich am angegebenen Tag generiert.

    - **Bi-weekly**: Berichte werden alle zwei Wochen am angegebenen Tag generiert.

    - **Monthly**: Berichte werden monatlich am ersten Tag des Monats, am 15. des Monats oder am letzten Tag des Monats generiert.

2. Geben Sie einen Datumsbereich an:

    - **Reports include data up to the Start the schedule time specified below**: Das bedeutet, ein Bericht kann bis zu 23 Stunden mehr Daten enthalten. Während sich dies nur unwesentlich auf die wöchentlichen oder monatlichen Berichte auswirkt, können "tägliche" Berichte abhängig vom Beginn der Planungszeit die Daten von fast zwei Tagen enthalten.

    - **Reports include data up to 23:59:59 of the previous day**: Das bedeutet, dass die Datenerfassung für den Bericht erst kurz vor Mitternacht beendet

wird. Berichte mit einer genauen Zeitperiode (Beispiel: Tägliche Berichte enthalten 24 Stunden), jedoch ohne die absolut letzten Daten.

3. Geben Sie an, wann der Berichtzeitplan beginnen soll:

   - **Immediately**: Der Berichtzeitplan beginnt sofort nachdem der Bericht aktiviert wurde.

   - **Start on**: Der Berichtzeitplan beginnt am Datum und an der Uhrzeit, die in den betreffenden Feldern festgelegt ist.

   a. Geben Sie ein Datum in das Feld **mm/dd/yyyy** ein.

   b. Geben Sie eine Uhrzeit in die betreffenden Felder **hh** und **mm** ein.



Hinweis

Klicken Sie auf das Kalendersymbol neben dem Feld **mm/dd/yyyy**, um den Datumsbereich über den dynamischen Kalender festzulegen.

4. Klicken Sie auf **Next**.

Schritt 4: Geben Sie den Empfänger des Berichts an

Prozedur

1. Geben Sie eine Betreffzeile für die E-Mail-Nachricht mit dem Bericht in das Feld **Subject** ein.

2. Geben Sie eine Beschreibung des Berichts in das Feld **Message** ein.

3. Wählen Sie **Email the report as an attachment**, um den Bericht an den angegebenen Empfänger zu versenden.

4. Aktivieren Sie diese Option, um Benutzer oder Gruppen aus der Liste **Report Recipients** auszuwählen.

5. Wählen Sie die Benutzer/Gruppen, die den Bericht erhalten sollen, und klicken Sie auf die Schaltfläche **>>**.

6. Klicken Sie auf **Finish**, nachdem Sie alle Benutzer/Gruppen ausgewählt haben, die den Bericht erhalten sollen.



Anhang B

Überlegungen zur Verteilung

Dieser Anhang bietet einen Überblick über die Verteilungsplanung für Endpoint Encryption.



Hinweis

Informationen zur Durchführung eines Pilotprogramms vor der Verteilung finden Sie unter *Pilotverteilung von Endpoint Encryption auf Seite C-1*.

Es werden folgende Themen behandelt:

Checkliste für die erste Verteilung

Der Fragebogen unterstützt Sie bei der Definition des Projektteams, der Dokumentation der Betriebsumgebung, der Bewertung der Architekturanforderungen, der Ermöglichung der Prüfung von Desktop-Hardware- und -Software-Profilen und der Definition von Sicherheitsfragen und administrativen bzw. Support-Prozessen.

TABELLE B-1. Checkliste für die erste Verteilung

ELEMENT ODER OBJEKT	FRAGEN
Endbenutzer	1. Für wie viele Benutzer soll die Verteilung insgesamt durchgeführt werden? 2. Wie viele davon sind: • Unternehmensadministrator • Gruppenadministrator • Authentifizierer (Helpdesk-Mitarbeiter) • Endbenutzer
Endpunkte	1. Gibt es auf der Hardware eine Standard-Anzahl von Partitionen? 2. Besitzen die Geräte mehrere physische Festplatten? 3. Gibt es Geräte mit Dual-Boot-Managern? 4. Welche Standard-Software ist installiert? Prüfen Sie Folgendes: a. Virenschutz b. Sicherheitsanwendungen, die Software-Installationen blockieren c. Frühere Verschlüsselungsprodukte

ELEMENT ODER OBJEKT	FRAGEN
Unternehmensnetzwerke und -datenbanken	1. Wie viele PolicyServer Instanzen werden zur Unterstützung der Benutzerbasis erforderlich sein? a. Schätzen Sie die maximale Benutzeranzahl für die nächsten drei Jahre. b. Falls die Domänenauthentifizierung verwendet wird, ist ein PolicyServer für jede Active Directory-Domäne erforderlich. 2. Ist eine Lastverteilung auf den Servern erforderlich? a. Die Lastverteilung wird für Installationen empfohlen, die Redundanz und hohe Verfügbarkeit für PolicyServer verlangen. b. Es kann Clustering verwendet werden, um Redundanz und hohe Verfügbarkeit für die Datenbankserver zu bieten. 3. Wie lauten die Schätzungen für die Datenbankgröße? a. Schätzen Sie die maximale Benutzeranzahl für die nächsten drei Jahre. b. Der Speicherplatzbedarf beträgt etwa 1 GB pro Jahr je 1.000 Endbenutzer. 4. Werden Agents erforderlich sein, um über das Internet mit dem PolicyServer zu kommunizieren? a. Fragen Sie beim internen Netzwerk-/ Sicherheits-Team nach, um die Anforderungen für das Verfügbarmachen eines Webservers im Internet zu verstehen. b. Folgendes wird mit einem von außen erreichbaren PolicyServer vollständig unterstützt: • Domänenauthentifizierung/Single Sign-On kann über das Internet verwendet werden • Richtlinien-Updates über das Internet • Geräte-Auditing über das Internet • Online-Kennwortzurücksetzung

Checkliste für die Sicherheitsinfrastruktur

Überprüfen Sie die bestehende Sicherheitsinfrastruktur, bevor Sie einen neuen IT-Dienst in der Produktionsumgebung verteilen. Trend Micro bietet eine Checkliste für die Sicherheitsinfrastruktur, die die Punkte enthält, die in folgenden Bereichen überprüft werden sollten:

- Endbenutzer
- Reaktion auf Vorfälle
- Risikobewertung
- Personalabteilung
- Einhaltung von Richtlinien

Weitere Informationen finden Sie unter *Checkliste für die Sicherheitsinfrastruktur auf Seite B-4*.

Checkliste für die Sicherheitsinfrastruktur

In der folgenden Tabelle werden die Fragen beschrieben, die Sie zur vorhandenen und potenziellen Sicherheitsinfrastruktur stellen sollten, um besser zu verstehen, wie sich die Verteilung von Endpoint Encryption auf das Unternehmen auswirken wird.

TABELLE B-2. Checkliste für die Sicherheitsinfrastruktur

PRÜFEN	FRAGEN
Endbenutzer	1. Enthält die Endbenutzerschulung die neuen Funktionen von Endpoint Encryption? 2. Wurde die Richtlinie zur akzeptablen Nutzung (Acceptable Use Policy, AUP) aktualisiert, so dass sie Verschlüsselungsdienste einschließt, insbesondere Strafen für die Nichtverwendung oder Umgehung der Verschlüsselung? 3. Werden Benutzer benachrichtigt, wenn sie sich bei einem Endpunkt anmelden, der auf die AUP hinweist? 4. Wurden alle Benutzer umfassend darin geschult, wie man den Verlust oder Diebstahl eines Geräts meldet? 5. Wurden die Benutzer in den Verfahren hinsichtlich fehlgeschlagener Anmeldeversuche und der Kennwortwiederherstellung geschult? 6. Gibt es eine Richtlinie für die Verschlüsselung vertraulicher Dokumente, die aus dem Unternehmen hinaus gesendet werden? 7. Wurden der AUP neue Kennwortrichtlinien hinzugefügt?
Reaktion auf Vorfälle	1. Wurde die Richtlinie für die Reaktion auf Vorfälle (Incident Response, IR) aktualisiert, so dass sie die bei Verlust oder Diebstahl eines Geräts durchzuführenden Aktionen einschließt? 2. Wurde für die PolicyServer Protokolle ein Zeitplan für die Prüfung der Audit-Protokolle festgelegt? 3. Wurden die E-Mail-Warnungen einschließlich der Empfänger und der erwarteten Reaktion beim Empfang eines Alarms zur IR-Richtlinie hinzugefügt? 4. Wurden bestimmte Kriterien dafür entwickelt, dass ein Gerät ausgelöscht oder per Wipe gelöscht werden darf, einschließlich der Audit-Trail-Dokumentation nach der Durchführung der Aktion?

PRÜFEN	FRAGEN
Risikobewertung	1. Wurde eine neue Risikobewertung durchgeführt, um die von Endpoint Encryption gebotene Änderung des Risikoprofils zu zeigen? 2. Wurden die Risikobewertungsverfahren aktualisiert, so dass sie die vom PolicyServer bereitgestellten Audit-Daten einschließen?
Notfall-Wiederherstellung	1. Wurde der PolicyServer zur Liste der kritischen Dienste hinzugefügt? 2. Wurde der Plan zur Notfall-Wiederherstellung aktualisiert, so dass er die Wiederherstellung des PolicyServer Dienstes einschließt? 3. Wurde ein Verfahren entwickelt, das die Wiederherstellung der auf einem Gerät gespeicherten Benutzerdaten ermöglicht?
Personalabteilung	1. Wurde die Checkliste für neue Mitarbeiter aktualisiert, so dass sie alle neuen Prozesse für Endpoint Encryption enthält? 2. Wurden die Prozesse bei Beendigung des Arbeitsverhältnisses aktualisiert, so dass sie alle neuen Prozesse für Endpoint Encryption enthalten – insbesondere das Auslöschen/Wipe von Geräten?
Einhaltung von Richtlinien	1. Wurde das Konformitätsprofil aktualisiert, so dass es die von Endpoint Encryption gebotenen Vorteile enthält? 2. Wurde eine Konformitätsprüfung für alle Aspekte der Implementierung und Verteilung von Endpoint Encryption durchgeführt?

Richtlinien und Sicherheitsprofile erstellen

Trend Micro Endpoint Encryption verfügt über Standard-Sicherheitsrichtlinien, die im Hinblick auf die Verteilungs- und Schutzziele geprüft werden sollten. Neben weiteren Standard-Richtlinieneinstellungen gibt es Standard-Richtlinien für den Benutzernamen, die Kennwortkomplexität und Änderungsanforderungen, die Gerätesteuerung, die Richtliniensynchronisierung, die Gerätesperre und den Geräte-Wipe. Standard-Richtlinien können abhängig von den Sicherheitszielen und den Anforderungen

hinsichtlich der Einhaltung von Gesetzesvorschriften zum Datenschutz einfach geändert werden.

Wenn Sie Endpoint Encryption zur Steuerung von Wechseldatenträgern einsetzen, können Sie Entscheidungen zu den zulässigen USB-Medien treffen. Sie können festlegen, wann und wo diese benutzt werden können (innerhalb und außerhalb des Netzwerks, jederzeit), um sicherzustellen, dass Benutzer die Sicherheitsrichtlinien und Ziele einhalten.

Im *Endpoint Encryption Administratorhandbuch* finden Sie eine vollständige Beschreibung der Richtlinien, Standardwerte und konfigurierbaren Optionen.



Hinweis

Wenn Endpoint Encryption zum Verwalten von Richtlinien und Wechselmedien verwendet wird:

- Testen und validieren Sie vor der Verteilung die Richtlinienvorlagen.
- Entscheiden Sie, welche USB-Geräte und Wechselmedien erlaubt sind und wann und wo diese verwendet werden können (im Netzwerk, außerhalb des Netzwerks oder beides), um sicherzustellen, dass die Benutzer die Sicherheitsvorgaben einhalten.

Überlegungen zur Änderungsverwaltung

PolicyServer und die dazugehörigen Datenbanken sind unternehmenskritische Dienste. Überlegungen zum Änderungsmanagement tragen dazu bei, die Verfügbarkeit für Endbenutzer sicherzustellen, die versuchen, sich beim Netzwerk zu authentifizieren. Wenn Änderungen erforderlich sind:

- Überwachen Sie aktiv die CPU-Auslastung und legen Sie einen Schwellenwert dafür fest, wann der PolicyServer Windows-Dienst neu gestartet werden sollte.
- Starten Sie den Dienst regelmäßig gemäß einem Zeitplan entsprechend neu, der in etablierten Wartungsfenster des Unternehmens passt (täglich, wöchentlich, monatlich).
- Starten Sie den PolicyServer Windows Dienst immer dann neu, wenn Wartungsmaßnahmen für die Active Directory-Umgebung, den Server, die Datenbank oder zugehörige Kommunikation durchgeführt werden.

- Sichern Sie regelmäßig die PolicyServer Datenbanken, genau wie alle anderen unternehmenskritischen Datenbanken.
- Es wird empfohlen, primäre Datenbanken und Protokolldatenbanken nachts zu sichern und die Sicherungen in einem anderen Gebäude aufzubewahren.



Warnung!

Alle Änderungen an den Active Directory- oder Datenbank-Umgebungen können die Verbindung zum PolicyServer beeinträchtigen.

Installationsvoraussetzungen für Full Disk Encryption

Das Installationsprogramm von Full Disk Encryption überprüft automatisch das Zielsystem, um sicherzustellen, dass alle erforderlichen Systemvoraussetzungen vor der Installation des Agent erfüllt sind. Beim Erkennen einer Systeminkompatibiltität wird das Installationsprogramm geschlossen und am selben Speicherort wie das Installationsprogramm wird der Text `PreInstallCheckReport.txt` generiert.

Ermitteln Sie anhand der Installations-Checkliste, welche Systemvoraussetzungen nicht erfüllt werden. Die Checkliste befindet sich im selben Ordner wie das Installationsprogramm von Full Disk Encryption.

TABELLE B-3. Vom Installationsprogramm überprüfte Bedingungen

SPEZIFIKATION	VORAUSSETZUNG	BESCHREIBUNG
Unterstütztes Betriebssystem	Nicht alle Betriebssysteme werden unterstützt	Full Disk Encryption kann nicht unter bestimmten Versionen von Windows installiert werden.

Spezifikation	Voraussetzung	Beschreibung
Die Encryption Management for Microsoft BitLocker ist bereits installiert.	Kein anderes Programm zur Festplattenverschlüsselung darf installiert sein.	Die Encryption Management for Microsoft BitLocker darf nicht installiert sein. Deinstallieren Sie die Encryption Management for Microsoft BitLocker, um Full Disk Encryption zu installieren, oder verwenden Sie stattdessen die Encryption Management for Microsoft BitLocker.
Feste Medien	Interne Festplatte	Full Disk Encryption kann nicht auf Wechseldatenträgern installiert werden, auf denen Windows ausgeführt wird.
Mehrere Festplatten	Nur eine Festplatte ist zulässig.	Auf dem Endpunkt darf sich nur eine Festplatte befinden. Umgebungen mit mehreren Festplatten werden nicht unterstützt.
Freier Speicher	Mindestens 256MB	
Arbeitsspeicher	Mindestens 512MB 1GB empfohlen	
Partitionsanzahl	Weniger als 25 Partitionen	Partitionen mit erweiterten MBRs sind nicht verfügbar.
Partitionstyp	Nur MBR wird unterstützt	GUID-Partitionstabelle (erforderlich für Festplatten, die größer als 2 TB sind) wird gegenwärtig nicht unterstützt.
Physisches Laufwerk ist bootfähig	Eine bootfähige Partition ist erforderlich.	Full Disk Encryption muss auf einer bootfähigen Partition installiert werden.

SPEZIFIKATION	VORAUSSETZUNG	BESCHREIBUNG
SCSI-Festplatte	ATA-, AHCI- oder IRRT-Festplattencontroller. SCSI wird nicht unterstützt.	• Die Prüfung gibt nur eine Warnung aus, da Windows ein SATA-Laufwerk möglicherweise als SCSI-Laufwerk meldet. • Wenn es sich bei der Festplatte nicht um echtes SCSI-Laufwerk handelt, kann Full Disk Encryption installiert werden. Wenn Sie sich nicht sicher sind, nehmen Sie eine physische Überprüfung des Laufwerks vor.
Microsoft .Net Framework	.NET 2.0 SP1 oder neuer ist erforderlich für Windows XP oder früher.	Wird für Windows Vista oder neuere Betriebssysteme weggelassen.
SED-Hardwarekompatibilität BitLocker ist aktiviert	Hardware-Verschlüsselung ist aktiviert, falls vorhanden. BitLocker muss deaktiviert sein.	Full Disk Encryption unterstützt momentan Seagate™ DriveTrust™ und OPAL-kompatible Laufwerke. Full Disk Encryption und BitLocker können nicht gleichzeitig für die Festplattenverschlüsselung verantwortlich sein.



Hinweis

Wenn die Präinstallationsprüfung aus einem dieser Gründe fehlschlägt, wenden Sie sich für weitere Hilfe an Trend Micro.

Beispielbericht zur Präinstallationsprüfung

```
Trend Micro Full Disk Encryption Prüfungen vor der Installation
 ------------------------------
Name:     Test des unterstützten Betriebssystems
Beschreibung:    Überprüft das unterstützte Betriebssystem.
Status:      Übergehen
 ------------------------------
Name:     Feste Medien
Beschreibung:    Überprüft, ob die physische Festplatte fest
                installiert ist (kein Wechselmedium).
Status:      Übergehen
 ------------------------------
Name:     Freier Speicher
Beschreibung:    Überprüft, ob die Festplatte über genügend
                freien Speicherplatz verfügt.
Status:      Übergehen
 ------------------------------
Name:     Arbeitsspeicher
Beschreibung:    Überprüft, ob genügend RAM zum Ausführen
                von Trend Micro Full Disk Encryption
                verfügbar ist.
Status:      Übergehen
 ------------------------------
Name:     Partitionsanzahl
Beschreibung:    Überprüft, ob die Festplatte nicht über
                zu viele Partitionen verfügt.
Status:      Übergehen
 ------------------------------
Name:     Partitionstyp
Beschreibung:    Überprüft, ob die Festplatte mit einer
                kompatiblen Partitionierungsmethode
                partitioniert wurde.
Status:      Übergehen
 ------------------------------
Name:     PhysicalDrive ist startbar
Beschreibung:    Überprüft, ob PhysicalDisk0 die
                Boot-Partition enthält.
Status:      Übergehen
 ------------------------------
Name:     SCSI-Festplatte
```

```
Beschreibung:    Überprüft, ob es sich um eine SCSI-Festplatte
                handelt.
Status:      Warnung
 ------------------------------
Name:     .Net Framework-Runtime
Beschreibung:    Überprüft, ob die .NET-Runtime-Version
                mindestens 2.0 (SP1) ist.
Status:      Überspringen
 ------------------------------
Name:     SED-Hardwarekompatibilität
Beschreibung:    Überprüft, ob der Computer über
                SED-Hardwarekompatibilität verfügt
Status:      Überspringen
 ------------------------------
Name:     BitLocker ist nicht installiert
Beschreibung:    Überprüft, ob auf dem Gerät BitLocker
                installiert ist.
Status:      Übergehen
```

Endbenutzer-Kommunikation

Um die Auswirkungen auf die Produktivität der Benutzer zu begrenzen und den Wechsel auf eine sichere Verschlüsselung zu erleichtern, definieren Sie einen Kommunikationsplan für die Endbenutzer, um diese vorzuwarnen. Die Kommunikation nach der Verteilung spielt ebenfalls eine wichtige Rolle für den reibungslosen Einstieg in die Verwendung von Trend Micro Endpoint Encryption.

Fragen an Endbenutzern, die beantwortet werden müssen

Ein häufiges Hindernis für die Akzeptanz im Unternehmen ist mangelnde Kommunikation. Für eine erfolgreiche Implementierung sind klare Informationen für Endbenutzer erforderlich. Dabei müssen drei Fragen beantwortet werden:

1. Warum benötigen wir Endpoint Encryption?

2. Wie unterstützt Endpoint Encryption mich und das Unternehmen?

3. Was wird sich ändern?

Vermitteln Sie Maßnahmen, Termine und Gründe

Trend Micro empfiehlt, dass die leitende Person des Datenschutzprojekts eine Nachricht an die Endbenutzer schickt, in der die Bedeutung des Projekts für das Unternehmen und die Vorteile für die Benutzer herausgestellt wird. In der Knowledge Base befinden sich mehrere Vorlagen für die Endbenutzer-Kommunikation, die vor der Verteilung von Endpoint Encryption benutzt und an Ihre Kommunikationsanforderungen angepasst werden können.

Einführung der Änderung

1. Einen Monat vor dem Rollout sollte eine Person aus dem Management beschreiben, warum die neue Software-/Hardware-Verschlüsselung eingeführt wird und welche Vorteile für die Endbenutzer und das Unternehmen durch die Einhaltung der neuen Prozesse entstehen.
2. Teilen Sie den Benutzern einen Zeitplan für den Rollout mit, und informieren Sie sie darüber, wie es nach Tag 1 weitergeht und wie sie Hilfe zur neuen Software erhalten können.

Kommunikation eine Woche vor dem Rollout

1. Wiederholen Sie, welche Änderungen kommen werden und was die Benutzer an dem Tag erwartet, an dem die neuen Authentifizierungsverfahren auf ihren Endpunkten erforderlich sind.
2. Fügen Sie Screenshots und detaillierte Anweisungen zu den Konventionen für Benutzernamen oder Kennwörtern und zu anderen internen Support-Diensten hinzu.

Kommunikation am Tag vor dem Rollout

1. Bekräftigen Sie das Timing des Rollout-Zeitplans, welche Erwartungen erfüllt werden und an wen man sich zur Unterstützung wenden kann.

2. Verteilen Sie Merkzettel und Helpdesk-Informationen, und geben Sie Kontaktinformationen für den Ansprechpartner vor Ort an, der verfügbar ist, um am nächsten Tag die Benutzer zu unterstützen.

Kommunikation nach dem Rollout

1. Wiederholen Sie die Helpdesk-Informationen, und geben Sie die Kontaktinformationen für den Ansprechpartner vor Ort an, der verfügbar ist, um am nächsten Tag die Benutzer zu unterstützen.
2. Stellen Sie Tools zur Unterstützung der Fehlerbehebung bereit.



Anhang C

Pilotverteilung von Endpoint Encryption

In diesem Anhang wird die Ausführung eines Pilotprogramms vor der Verteilung von Endpoint Encryption im gesamten Unternehmen beschrieben. Trend Micro empfiehlt das Ausführen eines Pilotprogramms und die Durchführung einer Testverteilung an eine kleine Gruppe von Benutzern, bevor die Verteilung an ein größeres Publikum erfolgt.



Hinweis

Informationen zu allgemeinen Überlegungen zur Verteilung finden Sie unter *Überlegungen zur Verteilung auf Seite B-1*.

Es werden folgende Themen behandelt:

Info über Pilotprogramme

Ein Pilotprogramm ermöglicht einem Unternehmen, die Installationsmethode, die bei der Installation von Endpoint Encryption angewendet werden soll, endgültig festzulegen. Die effektivsten Pilotprogramme schließen verschiedene Abteilungen, Zielbenutzer und Geräte ein. Wenn das Unternehmen beispielsweise zehn verschiedene Laptop-Hersteller unterstützt, sollte jedes dieser Geräte in das Pilotprogramm aufgenommen werden. Ebenso sollten, wenn bestimmte wichtige Gruppen speziell betroffen sind, ein oder zwei Mitglieder der Gruppe(n) am Pilotprogramm teilnehmen.

Projektteam zuweisen

Zu der erfolgreichen Implementierung gehören die Gewährleistung der Kontinuität sowie das Erzielen der Akzeptanz durch die internen Benutzer. Wenn das Team so strukturiert wird, dass es ein oder mehrere strategische Mitglieder aus den von der Software-Verteilung betroffenen Abteilungen umfasst, kann dies das Erzielen eine Akzeptanz unterstützen und die Führungsstärke des Projektteams erhöhen. Es wird empfohlen, dass Ihr Projektteam ein oder mehrere Mitglieder aus jeder der folgenden Gruppen umfassen sollte:

- Geschäftsleitung
- Anwendungsserver des Unternehmens
- Datenbank-Administratoren des Unternehmens
- Datensicherheit
- Desktop-Unterstützung
- Notfall-Wiederherstellung

Strategie eines schrittweisen Rollout implementieren

Wenn das Pilotprogramm erfolgreich war, beginnen Sie mit dem Verteilen des Programms, indem Sie schrittweise auf jeweils 25 bis 50 Endpunkt-Clients mit der

Produktionsverteilung der Lösung beginnen. Stellen Sie sicher, dass sich einen Tag nach der Installation der neuen Lösung die Entwicklungsingenieure bei der ersten Bereitstellungsgruppe vor Ort befinden, damit unmittelbar Hilfe geleistet werden kann. Verteilen Sie die Lösung aufbauend auf den Erfahrungen der anfänglichen Gruppe von Agents auf 100 bis 200 Agents pro Nacht. Während die Verteilungsmethode weiter in der Produktionsumgebung validiert wird und wenn die internen IT- und Helpdesk-Teams zustimmen, ist es möglich, Tausende von Geräten für die gleichzeitige Verteilung festzulegen.

Checkliste für das Endpoint Encryption Pilotprogramm

Checkliste für das Pilotprogramm	Datum	Hinweise
Erforderliche Konfiguration von PolicyServer durchgeführt • Richtlinien festgelegt • Gruppen erstellt • Benutzer erstellt/importiert		
Client-Software installiert (Full Disk Encryption und/oder File Encryption) • Software lokal auf den Computer kopiert und ausgeführt		
Administrator, Authentifizierer und Benutzerkonten können auf Grundlage der Richtlinieneinstellungen auf Geräte zugreifen • Festes Kennwort • Single Sign-On • SmartCard		

Checkliste für das Pilotprogramm	Datum	Hinweise
Alle Computer sind mit der neuen Software kompatibel • Preboot-Authentifizierung und/ oder Verbindung bestätigt • Verschlüsselung wird abgeschlossen • Computer funktioniert normal • Dateien/Ordner gemäß Richtlinie verschlüsselt • USB-Port wird gemäß der Richtliniendefinition gesteuert • Warnungen, Ereignisprotokolle und Berichte von PolicyServer bestätigen die Administrator- und Endbenutzer-Aktivität		
Endbenutzer können Aktivitäten des Tagesgeschäfts durchführen • Mit dem bestehenden Benutzernamen/Kennwort oder SSO aus Preboot auf Windows zugreifen • Der Computer funktioniert innerhalb und außerhalb des Netzwerks normal • Der Benutzer kann auf alle Benutzerdaten, Anwendungen und Netzwerkressourcen zugreifen		

Checkliste für das Pilotprogramm	Datum	Hinweise
Systemadministratoren testen Support-Prozesse • Backup-Administratorkonten erstellen • Berichterstellung und Warnungen testen • Full Disk Encryption Recovery Console zum Sichern und Wiederherstellen von Dateien verwenden • Full Disk Encryption Recovery CD zum Entschlüsseln des Geräts und Entfernen des • Preboot-Authentifizierungsprozesses für die Remote-Hilfe verwenden • Gerätesperre und Geräte-Wipe testen.		



Anhang D

Endpoint Encryption Dienste

In der folgenden Tabelle werden alle Endpoint Encryption Dienste beschrieben. Die Informationen vermitteln ein Verständnis darüber, welche Dienste welche Endpoint Encryption Agents bzw. Funktion steuern und wie Sie ein Problem lösen.

TABELLE D-1. Endpoint Encryption Dienste

BETRIEBSSYSTEM	DIENST- ODER DAEMON-NAMEN	ANZEIGENAME	BESCHREIBUNG	DATEINAME
PolicyServer	PolicyServer Windows-Dienst	PolicyServer Windows-Dienst	Verwaltet die Kommunikation zwischen Endpoint Encryption Diensten und Datenbanken.	`PolicyServer WindowService.exe`
	TMEE Dienst	Endpoint Encryption Dienst	Verwaltet die Kommunikation zwischen Endpoint Encryption Agent 5.0 (und höher) über einen verschlüsselten Kanal (RESTful).	`TMEEService.exe`
	IIS/ MAWebService2	Legacy Web-Service	Verwaltet die Kommunikation zwischen Endpoint Encryption Agent 3.1.3 (und älter) über einen verschlüsselten Kanal (SOAP).	n. v.
	TMEEForward	TMEEForward	Leitet den Datenverkehr von Endpoint Encryption 5.0 Patch 1 Agents zu PolicyServer weiter.	TMEEForward.exe
	TMEEProxyWindowsService	PolicyServer LDAProxy-Windows-Dienst	Bietet sichere Kommunikation zwischen Trend Micro PolicyServer und den Remote-LDAP-Servern.	`LDAProxyWindowsServices.exe`

Betriebssystem	Dienst- oder Daemon-Namen	Anzeigename	Beschreibung	Dateiname
Full Disk Encryption	DrAService	Trend Micro Full Disk Encryption	Bietet Sicherheit für Trend Micro Endpoint und die Verschlüsselung ganzer Festplatten.	`DrAService.exe`
Encryption Management for Microsoft BitLocker	FDE_MB	Trend Micro Full Disk Encryption, Encryption Management for Microsoft BitLocker	Gewährleistet Datensicherheit für Endpunkte mit Microsoft BitLocker	`FDEforBitLocker.exe`
Encryption Management for Apple FileVault	Daemon: TMFDEMM Agent: Trend Micro Full Disk Encryption	Trend Micro Full Disk Encryption, Encryption Management for Apple FileVault	Gewährleistet Datensicherheit für Endpunkte mit Apple FileVault.	
File Encryption	FileEncryption Service	Trend Micro File Encryption	Gewährleistet Trend Micro Endpunktsicherheit und Datenschutz für Dateien, Ordner und Wechselmedien.	`FEService.exe`



Anhang E

Glossar

In der folgenden Tabelle wird die Terminologie beschrieben, die in der gesamten Endpoint Encryption Dokumentation verwendet wird.

TABELLE E-1. Endpoint Encryption Terminologie

BEGRIFF	BESCHREIBUNG
Agent	Software, die auf einem Endpunkt installiert ist und die mit einem Verwaltungsserver kommuniziert.
Authentifizierung	Der Prozess des Identifizierens eines Benutzers.
ColorCode™	Die Authentifizierungsmethode, bei der eine Farbfolge als Kennwort eingegeben werden muss.
Command Line Helper	Ein Trend Micro Tool zum Erstellen von verschlüsselten Werten, um die Anmeldedaten zu sichern, wenn Installationsskripts für Endpoint Encryption Agents erstellt werden.
Command Line Installer Helper	Ein Trend Micro Tool zum Erstellen von verschlüsselten Werten, um die Anmeldedaten zu sichern, wenn Installationsskripts für Endpoint Encryption Agents erstellt werden.

BEGRIFF	BESCHREIBUNG
Control Manager	Der Trend Micro Control Manager ist eine zentrale Management-Konsole zur Verwaltung von Produkten und Services von Trend Micro auf Gateways, Mail-Servern, File-Servern und Unternehmensdesktops.
Domänenauthentifizierung	Die Authentifizierungsmethode, die Single Sign-On (SSO) mit Hilfe von Active Directory unterstützt.
DriveTrust™	Hardware-basierte Verschlüsselungstechnologie von Seagate™.
Encryption Management for Microsoft BitLocker	Der Endpoint Encryption Full Disk Encryption Agent für Microsoft Windows-Umgebungen, auf denen lediglich Microsoft BitLocker auf dem Hosting-Endpunkt aktiviert werden muss. Mit dem Encryption Management for Microsoft BitLocker Agent können Sie Endpunkte mit Trend Micro Full Disk Encryption in einer bestehenden Windows-Infrastruktur sichern. Weitere Informationen finden Sie unter *Info über Full Disk Encryption auf Seite 6-3*.
Encryption Management for Apple FileVault	Der Endpoint Encryption Full Disk Encryption Agent für Mac OS-Umgebungen, auf denen lediglich Apple FileVault auf dem Hosting-Endpunkt aktiviert werden muss. Mit der Encryption Management for Apple FileVault Agent können Sie Endpunkte mit Trend Micro Full Disk Encryption in einer bestehenden Mac OS-Infrastruktur sichern. Weitere Informationen finden Sie unter *Info über Full Disk Encryption auf Seite 6-3*.
Endpoint Encryption Gerät	Ein beliebiger Computer, ein Laptop oder ein Wechselmedium (externes Laufwerk, USB-Laufwerk), das von Endpoint Encryption verwaltet wird.

BEGRIFF	BESCHREIBUNG
Endpoint Encryption Dienst	Der PolicyServer Dienst, der die gesamte Kommunikation mit Endpoint Encryption 5.0 Patch 1 Agents sicher verwaltet. Weitere Informationen finden Sie unter *Info über PolicyServer auf Seite 1-13*. Angaben zur Kommunikation von Endpoint Encryption 3.1.3 Agents und niedriger finden Sie unter Legacy Web Service.
Unternehmen	"Endpoint Encryption - Unternehmen" ist der eindeutige Bezeichner für das Unternehmen in der PolicyServer Datenbank, der bei der Installation von PolicyServer konfiguriert wurde. Eine PolicyServer Datenbank darf mehrere Unternehmenskonfigurationen haben. Jedoch darf es in Endpoint Encryption Konfigurationen mit Control Manager nur ein Unternehmen geben.
File Encryption	Der Endpoint Encryption Agent für die Verschlüsselung von Dateien und Ordnern auf lokalen Laufwerken und Wechselmedien. Mit File Encryption können Sie die Dateien und Ordner auf nahezu jedem Gerät, das als Laufwerk im Host-Betriebssystem angezeigt wird, schützen. Weitere Informationen finden Sie unter *Info über die File Encryption auf Seite 6-4*.
FIPS	Federal Information Processing Standard. Der von der US-Regierung definierte Standard für Computersicherheit.
Festes Kennwort	Die Authentifizierungsmethode zur Verwendung herkömmlicher Benutzerkennwörter, die aus Buchstaben und/oder Ziffern und/oder Sonderzeichen bestehen.
Full Disk Encryption	Der Endpoint Encryption Agent für die Verschlüsselung von Hardware und Software mit Preboot-Authentifizierung.

BEGRIFF	BESCHREIBUNG
KeyArmor	Das mit Endpoint Encryption kennwortgeschützte und verschlüsselte USB-Laufwerk. **Hinweis** Endpoint Encryption 5.0 verfügt über keine KeyArmor Geräte. Es werden jedoch ältere KeyArmor Geräte unterstützt.
Legacy Web-Service	Der PolicyServer Dienst, der die gesamte Kommunikation mit Agents für Endpoint Encryption 3.1.3 und niedriger sicher verwaltet. Weitere Informationen finden Sie unter *Info über PolicyServer auf Seite 1-13*. Informationen zur Kommunikation mit Endpoint Encryption 5.0 Patch 1 finden Sie unter Endpoint Encryption Dienst.
OCSP	Online Certificate Status Protocol. Das Protokoll, das für digitale X.509- Zertifikate verwendet wird.
OfficeScan	OfficeScan schützt Unternehmensnetzwerke vor Malware, Netzwerkviren, webbasierten Bedrohungen, Spyware und kombinierten Bedrohungen. OfficeScan ist eine integrierte Lösung und besteht aus einem Agent am Endpunkt sowie einem Serverprogramm, das alle Agents verwaltet.
OPAL	Die Subsystemklasse für Sicherheit der Trusted Computing Group für Client-Geräte.
Kennwort	Alle Arten von Authentifizierungsdaten, die in Kombination mit einem Benutzernamen verwendet werden, wie feste Kennwörter, PINs und ColorCode.
PIN	Die Authentifizierungsmethode zur Verwendung einer PIN, die von Geldautomaten her bekannt ist.
PolicyServer	Der zentrale Verwaltungsserver, der die Richtlinien zur Verschlüsselung und Authentifizierung auf die Endpoint Encryption Agents verteilt.

Begriff	Beschreibung
Remote-Hilfe	Die Authentifizierungsmethode, um Endpoint Encryption Benutzer, die ihre Anmeldedaten vergessen haben, oder Endpoint Encryption Geräte, auf denen die Richtlinien nicht innerhalb eines festgelegten Zeitraums synchronisiert wurden, zu unterstützen.
Wiederherstellungskonsole	Die Benutzeroberfläche von Full Disk Encryption zur Wiederherstellung von Endpoint Encryption Geräten, wenn es zu einem Ausfall des primären Betriebssystems gekommen ist, Netzwerkprobleme untersucht werden und Benutzer, Richtlinien und Protokolle verwaltet werden.
Reparatur-CD	Die bootfähige CD von Full Disk Encryption, mit der ein Laufwerk entschlüsselt werden kann, bevor Full Disk Encryption entfernt wird, für den Fall, dass der Datenträger beschädigt wird.
RESTful	Representational State Transfer (Web-API). Das verschlüsselte AES-GCM-Kommunikationsprotokoll, das von Endpoint Encryption 5.0 Agents verwendet wird. Nachdem sich ein Benutzer authentifiziert hat, generiert PolicyServer ein Token im Zusammenhang mit der spezifischen Richtlinienkonfiguration. Ohne Authentifizierung verweigert der Dienst alle Richtlinientransaktionen. **Hinweis** Informationen zu AES-GCM finden Sie unter: http://tools.ietf.org/html/rfc5084#ref-GCM%3F
RSA SecurID	Ein Mechanismus zum Ausführen der Zwei-Faktor-Authentifizierung für einen Benutzer bei einer Netzwerkressource.
SED	Secure Encrypted Device (sicher verschlüsseltes Gerät). Eine Festplatte oder ein anderes Gerät, das verschlüsselt wurde.
Selbsthilfe	Die Authentifizierungsmethode, um Endpoint Encryption Benutzer dabei zu unterstützen, Antworten auf Sicherheitsfragen zu geben, bevor der Technische Support bei einem vergessenen Kennwort kontaktiert wird.

Begriff	Beschreibung
Smartcard	Die Authentifizierungsmethode, bei der eine physische Karte zusammen mit einer PIN oder einem festen Kennwort erforderlich ist.
SOAP	Simple Object Access Protocol. Das verschlüsselte Kommunikationsprotokoll, das von allen Agents von Endpoint Encryption 3.1.3 (und älter) zur Kommunikation mit PolicyServer verwendet wird. In bestimmten Situationen erlaubt SOAP möglicherweise unsichere Richtlinientransaktionen ohne Benutzerauthentifizierung. Legacy Web Service filtert SOAP-Aufrufe, indem eine Authentifizierung erforderlich gemacht wird und die Befehle begrenzt werden, die SOAP akzeptiert.



Stichwortverzeichnis

R

S

T

U

V



TREND MICRO INCORPORATED

Trend Micro Deutschland GmbH Zeppelinstraβe 1 Hallbergmoos, Bayern 85399 Deutschland

Tel.: +49 (0) 811 88990-700 Fax: +4981188990799 info@trendmicro.com

www.trendmicro.de

Item Code: APGM56403/140410